思科系列丛书

Cisco 无线局域网配置基础

（第 2 版）

常　潘　徐　刚　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

VISIT…

LANZAROTE

Caliente.com

内 容 简 介

本书第 1 版没有涉及无线复杂的技术，仅以浅显易懂的文字讲述了无线局域网基础知识以及 Cisco 无线局域网的配置，第 2 版与第 1 版相比，增加了对 IEEE 802.11ac 及 Cisco FlexConnect 技术的介绍，重点讲述如何进行无线现场勘查，如何计算无线局域网的吞吐量；无线配置部分采用了 Cisco 最新的映像软件及 ACS 最新版。

本书先简单介绍无线局域网的接入点、协议、射频、蜂窝、以太网供电、IEEE 802.11 标准、WLAN 安全、用户端设备关联及漫游和信道选择等无线网络基础知识；接下来详细介绍 Cisco 统一无线网络的架构、轻量级 AP 同无线控制器的关联、用户数据的传递以及如何在多个不同的 AP 间进行漫游，重点介绍 Cisco 无线设备不同于其他厂商设备的特殊功能配置，包括 HREAP、FlexConnect、IEEE 802.11n、IEEE 802.11ac、Mesh、非法 AP 的检测以及多控制器之间的负载均衡；本书通过实例讲述了无线网络用户的认证以及如何使用 Cisco 无线网络管理系统对无线设备、资源及用户进行全方位的管理；介绍了无线现场勘察的相关知识。

本书既可作为思科网络技术学院的实验教材，也可供高等院校计算机专业的高年级本科生或研究生使用，还可作为网络工程师的培训教材和网络管理人员的技术参考书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

Cisco 无线局域网配置基础 / 常潘，徐刚编著. —2 版. —北京：电子工业出版社，2014.7
（思科系列丛书）

ISBN 978-7-121-23789-8

Ⅰ. ①C… Ⅱ. ①常… ②徐… Ⅲ. ①无线网—局域网—配置—基本知识 Ⅳ. ①TN925-62

中国版本图书馆 CIP 数据核字（2014）第 153682 号

策划编辑：宋　梅
责任编辑：宋　梅
印　　刷：
装　　订：
出版发行：电子工业出版社
　　　　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×980　1/16　印张：16.5　字数：370 千字
版　　次：2011 年 3 月第 1 版
　　　　　2014 年 7 月第 2 版
印　　次：2014 年 7 月第 1 次印刷
印　　数：4 000 册　　定价：49.90 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

自 2000 年初出现 WLAN 技术以来，WLAN 技术和应用得到了快速的发展，特别是近几年来，随着一系列新的 IEEE 802.11 标准的制定完成以及移动智能终端的大量普及，个人、企业及运营商也越来越依赖通过移动无线技术，特别是 WLAN 技术实现各种个人及商业应用。

从 WLAN 技术发展之初至今，思科作为 WLAN 设备的提供商就一直伴随着这个市场一同成长，也一直是企业级 WLAN 设备的主要生产厂商。目前，全球大多数企业均选择采用思科的 WLAN 产品作为其无线网络的基础平台。

据有关调查显示，在未来几年里，全球将新增数十亿移动上网终端，这也意味着无线网络厂商将必须满足数十亿终端通过 WLAN 设备无线上网的需求。作为未来无线网络技术的生力军，在校师生非常有必要学习和了解全球最新无线网络技术，并有机会操作最新无线网络设备。

为了让广大在校师生可以了解并且熟悉思科的无线技术原理、产品特性及配置过程，我们特别邀请了常潘老师帮助编写完成了《Cisco 无线局域网配置基础》。常潘老师拥有多年教学经验，并对无线技术原理及厂商设备有着深刻的理解。由于思科软 / 硬件的升级，《Cisco 无线局域网配置基础》中的很多配置在高版本中已经逐步采用其他方式完成，此次我们特别邀请常潘老师对本书进行改版，增加了思科最新软件版本的配置实例及无线现场勘察等方面的内容，编写完成了《Cisco 无线局域网配置基础（第 2 版）》。

通过学习本教材，相信读者可以深入理解 WLAN 技术原理，并且具有一定设计、部署 WLAN 网络的实践能力；本教材可以作为高级院校师生学习 WLAN 技术的指导教材，并具有广泛的推广意义。

最后，在这里我们也感谢所有对该教材的成功出版发行作出贡献的同仁们。

思科大中华区无边界网络事业部高级总监

于 2014 年 5 月

前　言

在无线局域网普及之前，用户只能通过电缆将计算机连接到网络上，因此用户只能在室内使用计算机，这在很大程度上限制了用户的移动性，无线局域网的出现使用户摆脱了电缆的束缚。如今在任何无线网络覆盖的范围内，配备无线网卡的用户无论何时何地都能同网络保持连接。

本书主要帮助用户掌握无线局域网射频、安全、架构以及漫游方面的一些基础知识，在领会这些知识的基础上，详细讲述了 Cisco 统一无线局域网的配置。

本书共 7 章。

第 1 章讲述无线局域网的基础知识，包括无线局域网协议与组成部分，介绍了无线射频工作的原理以及无线局域网的几个标准，同时对以太网络供电进行了简单描述。

第 2 章讲述无线网络的架构及设计，介绍了无线局域网的安全认证及授权方式、AP 的蜂窝及用户漫游。

第 3 章讲述 Cisco 统一无线网络组成、架构及轻量级 AP 与控制器的关联及数据流的传递，以及用户如何在多个 AP 之间实现无缝漫游。

第 4 章讲述 Cisco 无线局域网的建立与配置，包括无线网络控制器的初始化，如何配置一个简单的 WLAN，详细讲述了如何配置 HREAP、IEEE 802.11n 及 Mesh 网络，如何管理射频资源以及在多个控制器之间实现负载均衡，如何检查网络中非法 AP 的存在。

第 5 章讲述如何对无线局域网用户进行认证，采用本地、RADIUS 及 LDAP 服务对用户进行认证，如何创建 Guest 账户。

第 6 章讲述如何采用 Cisco 无线网络管理软件 WCS 对无线资源及设备进行集中管理。

第 7 章讲述无线现场勘查等方面的知识，使读者对无线的部署能够有一定的了解。

为了方便用户进行配置，在附录中介绍了 Cisco 自主 AP 及轻量级 AP 之间的转换，轻量级 AP 到控制器的注册过程，如何在 Windows 中创建 DHCP 的 Option，让轻量级 AP 自动发现控制器；还介绍了轻量级 AP 的 Console 口维护与配置。

本书既可作为思科网络技术学院的实验教材，也可供高等院校计算机专业的高年级本科生或研究生使用，还可作为网络管理人员的技术参考书。在本书编写过程中，得到了华东师范大学网络中心徐刚老师的大力支持与帮助，他采用 Cisco 最新版本的软件更新了本书第 4～6 章中的配置及插图。本书还引用了网上很多公开的资料，在此向资料的作者表达谢意。由于作者水平有限及时间仓促，书中难免存在错漏之处，请广大读者批评指正。

编著者

2014年5月

目　录

第 1 章　无线局域网基础 ········ 1
1.1　无线局域网概述 ········ 2
1.1.1　冲突避免的无线局域网协议 ········ 2
1.1.2　WLAN 的组成部分 ········ 5
1.1.3　接入点的工作原理 ········ 6
1.1.4　无线局域网蜂窝 ········ 8
1.2　无线射频简介 ········ 10
1.2.1　RF 的工作原理 ········ 10
1.2.2　RF 的特征 ········ 11
1.2.3　描述 RF 信号强度的术语 ········ 16
1.2.4　WLAN 天线 ········ 19
1.3　WLAN 标准 ········ 21
1.3.1　管理机构 ········ 21
1.3.2　WLAN 帧类型和长度 ········ 22
1.3.3　IEEE 802.11b ········ 22
1.3.4　IEEE 802.11g ········ 24
1.3.5　IEEE 802.11a ········ 25
1.3.6　IEEE 802.11n ········ 25
1.3.7　IEEE 802.11ac ········ 31
1.3.8　其他 IEEE 802.11 标准 ········ 32
1.4　以太网供电 ········ 32
1.4.1　PoE 的工作原理 ········ 33
1.4.2　检测需供电的设备 ········ 33
1.4.3　向设备供电 ········ 34
1.4.4　配置 PoE ········ 38
1.4.5　查看 PoE ········ 38
第 2 章　无线网络架构及设计 ········ 40
2.1　WLAN 安全 ········ 41
2.1.1　以前的安全性 ········ 42
2.1.2　基于 EAP 的安全方法 ········ 43

2.1.3 WPA …… 44
2.1.4 WPA2 …… 45
2.1.5 无线认证方式总结 …… 46
2.2 AP 的关联和漫游 …… 46
2.2.1 漫游过程 …… 47
2.2.2 漫游的含义 …… 50
2.3 蜂窝布局和信道的使用 …… 50
2.3.1 确定 AP 蜂窝的大小 …… 50
2.3.2 WLAN 信道布局 …… 51
2.4 用户设备选型 …… 54
第 3 章 思科统一无线网络 …… 56
3.1 思科统一无线网络架构 …… 57
3.1.1 传统的 WLAN 结构 …… 57
3.1.2 Cisco 统一无线网络的组成 …… 58
3.1.3 WLC 功能 …… 61
3.1.4 轻量级 AP 的工作原理 …… 62
3.1.5 思科统一无线网络中的数据流格式 …… 63
3.2 轻量级 AP 的关联和漫游 …… 65
3.2.1 控制器内漫游 …… 66
3.2.2 控制器间漫游 …… 67
3.2.3 移动组 …… 70
3.2.4 静态 IP 漫游 …… 72
第 4 章 思科统一无线局域网的配置 …… 74
4.1 WLC 的基本配置 …… 75
4.1.1 WLC 的组成及接口 …… 75
4.1.2 配置相邻的接入交换机 …… 77
4.1.3 配置 Cisco 无线网络控制器 …… 77
4.1.4 进一步配置 WLC …… 79
4.1.5 配置 AP 组 …… 88
4.1.6 配置移动组 …… 91
4.2 配置 HREAP …… 93
4.2.1 CAPWAP 下 HREAP 的操作 …… 94
4.2.2 HREAP 的核心概念 …… 94

4.2.3 HREAP 的配置 ············ 96
4.2.4 FlexConnect ············ 101
4.3 管理无线射频资源 ············ 104
4.3.1 重写自动 RF 分组 ············ 106
4.3.2 重写动态 RRM ············ 107
4.3.3 频段选择 ············ 108
4.4 配置 IEEE 802.11n 网络 ············ 110
4.4.1 启用 IEEE 802.11n 的速率 ············ 110
4.4.2 配置 IEEE 802.11n 的无线局域网（WLAN） ············ 111
4.4.3 启用数据汇聚 ············ 112
4.4.4 40 MHz 和 80MHz 频宽操作 ············ 113
4.4.5 使用无线资源管理 ············ 114
4.4.6 使用静态无线资源管理 ············ 115
4.4.7 确认 IEEE 802.11n 和 IEEE 802.11ac 网络已运行 ············ 116
4.5 配置 Cisco Wireless Mesh 网络 ············ 116
4.5.1 思科 Mesh 无线架构 ············ 117
4.5.2 在网络中增加 Cisco Mesh AP ············ 121
4.5.3 配置 Mesh AP 的桥接模式 ············ 121
4.5.4 配置 Mesh AP 的角色 ············ 123
4.5.5 验证 Mesh 连接状态 ············ 124
4.5.6 设置全局 Mesh 参数 ············ 124
4.5.7 设置本地 Mesh 参数 ············ 125
4.5.8 配置以太网桥及 VLAN 标记 ············ 126
4.6 配置 LAP ············ 129
4.6.1 给 LAP 供电 ············ 129
4.6.2 配置连接 LAP 交换机端口 ············ 130
4.6.3 LAP 的初始配置 ············ 131
4.7 控制器冗余及 LAP 的负载均衡 ············ 133
4.7.1 控制器的物理端口及逻辑接口冗余 ············ 133
4.7.2 LAP 的负载均衡 ············ 135
4.7.3 使用 WLC 的 Web 界面配置 AP 的主、备、第三控制器 ············ 137
4.7.4 使用 WCS 配置 AP 的主、备、第三控制器 ············ 139
4.7.5 控制器冗余设计 ············ 139
4.7.6 快速 AP 故障转移 ············ 141
4.8 管理非法 AP ············ 143

4.8.1 配置 RLDP …… 145
4.8.2 定义非法 AP 的分类规则 …… 147
4.8.3 查看非法 AP …… 148
4.9 总结 …… 150

第 5 章 认证服务 …… 151

5.1 RADIUS 认证服务创建 …… 152
5.1.1 安装 ACS 服务器并配置 …… 152
5.1.2 在 WLC 上配置 RADIUS 服务器相关信息 …… 160
5.2 其他认证方式 …… 160
5.2.1 本地认证服务的创建 …… 160
5.2.2 LDAP 认证服务创建 …… 163
5.2.3 MAC 地址过滤 …… 163
5.2.4 配置 WLAN 使用各种认证服务 …… 169
5.3 创建 Guest 账户 …… 170
5.3.1 创建大堂大使账户 …… 171
5.3.2 使用大堂大使账户创建 Guest 账户 …… 171
5.3.3 配置有线来宾访问 …… 171

第 6 章 管理无线网络控制器 …… 175

6.1 WCS 及其配置 …… 176
6.1.1 WCS 简介 …… 176
6.1.2 使用 WCS 规划热图 …… 185
6.1.3 使用 WCS 查看接入用户的信息 …… 187
6.1.4 使用 WCS 自定义报表 …… 192
6.2 升级控制器软件 …… 194
6.2.1 使用 Web 管理页面升级 WLC 映像软件 …… 194
6.2.2 使用 CLI 命令端口升级控制器软件 …… 195
6.2.3 使用 WCS 升级控制器软件 …… 196
6.3 管理控制器配置文件 …… 197
6.3.1 从控制器上传配置文件 …… 198
6.3.2 存储配置文件 …… 199
6.3.3 使用 WCS 管理控制器的配置文件 …… 200
6.4 清除控制器配置文件 …… 201
6.4.1 采用 CLI 方式 …… 201

6.4.2 采用 Web 方式 …… 201
6.4.3 采用 WCS 方式 …… 201
6.4.4 删除控制器配置 …… 202
6.5 重新启动控制器 …… 202
6.5.1 通过 Web 方式重新启动 …… 202
6.5.2 通过 WCS 方式重新启动 …… 203
6.5.3 通过 CLI 方式启动 …… 203
第 7 章 无线现场勘察 …… 205
7.1 无线勘察概述及前期准备 …… 206
7.1.1 无线勘察的种类 …… 206
7.1.2 无线勘察的前期准备 …… 207
7.1.3 现场勘察事项的基本清单核对 …… 207
7.2 无线勘查的现场工作 …… 208
7.2.1 地图的校准 …… 208
7.2.2 信号的传播 …… 210
7.2.3 勘察路线 …… 210
7.2.4 信道扫描 …… 212
7.3 勘察后需验证的重点项目 …… 212
7.3.1 覆盖 …… 213
7.3.2 信道重叠 …… 214
7.3.3 信号噪声比 …… 214
7.3.4 本底噪声 …… 215
7.3.5 信号泄露和非法设备射频干扰 …… 216
7.3.6 使用无线控制器的链路测试功能协助评估覆盖 …… 217
7.4 无线网络的性能优化 …… 218
7.4.1 无线数据传输速率 …… 218
7.4.2 管理帧 …… 219
7.4.3 组播数据的传输 …… 220
附录 A Cisco 自主 AP 和轻量级 AP 之间的转换 …… 221
A.1 升级前的准备 …… 222
A.2 升级过程 …… 223
A.3 安装并运行升级工具必须满足的要求 …… 223
A.4 安装并运行升级软件 Upgrade Tool …… 224

A.5 IEEE 802.11n AP 的升级 225

附录 B LAP 的注册步骤 226

B.1 LAP 的注册步骤 227
B.2 第二层 CAPWAP 发现算法 227
B.3 第三层 CAPWAP 发现算法 228
B.4 WLC 的选举过程 233

附录 C Windows 2003 Server 中 DHCP Option 43 的创建 235

C.1 创建供应商类别 236
C.2 设置预定义的选项 238
C.3 定义 Option 43 选项 239

附录 D 采用 Console 口快速部署 LAP 241

D.1 配置 LAP 的登录用户名及密码 242
D.2 配置静态参数将 AP 注册到控制器 242
D.3 清除静态配置参数 243
D.4 删除 LAP 上的 CAPWAP 配置以便重新部署 243

附录 E IEEE 802.11 吞吐量的计算 244

E.1 无线网络传输开销分析 245
E.2 IEEE 802.11b 传输性能分析 246
E.3 IEEE 802.11a 传输性能分析 247
E.4 IEEE 802.11g 传输性能分析 247

附录 F 术语及缩略语 249

第 1 章



无线局域网基础

本章要点

- 无线局域网概述
- 无线射频简介
- WLAN 标准
- 以太网供电

1.1 无线局域网概述

现在社会的活动越来越依赖于计算机及计算机网络，随着各种移动设备如笔记本电脑、PDA、PAD 和 WiFi 手机等技术的日益成熟及普及，人们希望在移动中能够保持计算机网络的连通，但不希望受线缆的限制，能自由地变换这些移动设备的位置，在这种要求的推动下，产生了无线局域网（Wireless LAN，WLAN），无线局域网以自由空间的无线电波取代电缆中的电磁波或光缆中的光波进行数据传输，当前广泛使用的是符合 IEEE 802.11 标准的无线局域网，在下面的章节中，如果无特殊说明，所有的内容都是基于 IEEE 802.11 的无线局域网技术。

1.1.1 冲突避免的无线局域网协议

传统的以太网是由 IEEE 802.3 的标准定义的，每条以太网的链接都必须在严格的条件下运行，尤其是物理链路本身。例如，链路状态、链路速度和双工模式都必须符合标准的规定，无线局域网使用类似的协议，由 IEEE 802.11 标准定义。

有线以太网设备必须采用载波侦听多路访问 / 冲突检测（CSMA/CD）方法来传输和接收以太网帧。在共享的以太网网段上，计算机以半双工模式工作，每台计算机都可以先“发言”，然后侦听是否同其他正在发言的设备发生冲突。整个检测冲突的过程基于有线连接的最大长度，从网段的一端发送到另一端，检测到冲突之间的最大延迟是确定的。

在全双工或交换型以太网链路上，不存在冲突或争取带宽的问题，但它们必须遵循相同的规范。例如，在全双工链路上，必须在预期的时间内发送或接收以太网帧，这要求全双工双绞线的最大长度与半双工链路双绞线的最大长度相同。

虽然无线局域网也基于一组严格的标准，但无线介质本身难以控制，一般而言，当计算机连接到有线网络时，与其共享网络连接的其他设备的数量是已知的，而当计算机使用无线网络时，使用的传输介质为空气，由于接入层没有电缆和插口，因此无法限制其他最终用户使用相同频率无线电波。

无线局域网实际上是一种共享型网络，并且争用相同频率电波的主机数量不是固定的。在无线局域网中，冲突犹如家常便饭，因为每条无线连接都是半双工模式的。IEEE 802.11 WLAN 总是半双工模式的，因为传输站和接收站使用的频率相同。双方不能同时传输，否则将发生冲突。要实现全双工模式，必须在一个频率进行传输，在另一个频率进行接收，这类似于全双工以太网链路的工作原理，虽然这完全可行，但 IEEE 802.11 标准不允许采用全双工模式。

当多个无线工作站同时传输时，它们的信号将相互干扰，接收站收到的将是混乱的数据、噪声或错误信息。如果没有明确的方式来确定是否发生了冲突，传输站也无法知道发生了冲突，因为传输时将关闭其接收器。作为一个基本的反馈机制，每当无线工作站传输一帧后，接收工

作站必须发送一个肯定确认（Positive Acknowledgement），确认已正确地收到该帧。确认帧充当了基本的冲突检测工具，然而，它并不能预先防止冲突的发生。除广播帧与组播帧外，所有传送出去的帧必须得到响应，如图 1-1 所示，只要有任何一个环节失败，该帧将被认为已经丢失。

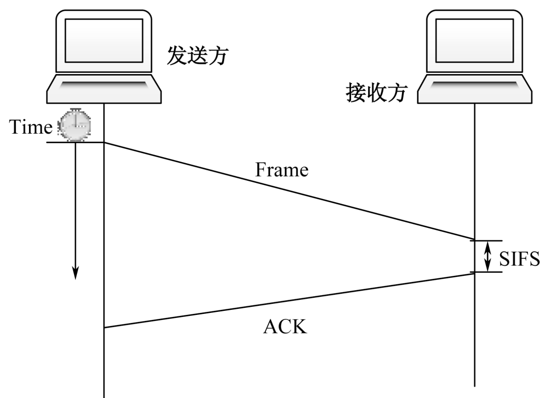


图 1-1　无线数据传输的肯定确认机制

图 1-1 所列的步骤称为原子操作，所有的步骤为一个整体，若没有完成所有的步骤，整个操作就视为失败，必须重传。

IEEE 802.11 标准使用一种名为载波侦听多路访问 / 冲突避免（CSMA/CA）的方法来避免冲突。注意，IEEE 802.3 有线网络是检测冲突，而IEEE 802.11 网络是尽可能避免冲突。

为实现冲突避免，要求所有工作站在传输每帧前进行侦听，当工作站有帧需要发送时，面临的将是下列情况之一：

① 没有其他设备在传输数据，工作站可立刻传输其帧，接收工作站必须发送一个确认帧，确认原始帧已在没有发生冲突的情况下到达。

② 另一台设备正在传输，工作站必须等待，等到当前帧传输完毕后，它再等待一段随机时间，然后传输自己的帧。

无线帧的长度不是固定的，当一个工作站传输其帧时，其他工作站如何知道该帧已传输完毕，可以使用无线介质呢？显然，工作站可以进行侦听，等待静默期的到来，但这样做并非总是有效的，其他工作站也在侦听，可能同时决定开始传输。IEEE 802.11 标准要求所有工作站在开始传输前等待一段时间，这段时间被称为 DCF 帧间间隔（DCF Interframe Space，DIFS）。

传输工作站可以在 IEEE 802.11 报头中包含一个持续时间值，以指出传输完当前帧所需的大概时间（网络分配矢量，Network Allocation Vector，NAV）。持续时间值包含传输完当前帧所需要的时隙数（单位通常为微秒），其他无线工作站必须查看持续时间值，并在考虑传输数据前等待相应的时间，直到 NAV 的值倒数至零，只要 NAV 的值不为零，就代表媒介处于忙碌状态，此为虚拟载波监听功能。当 NAV 为零时，虚拟载波侦听功能会显示媒介处于闲置状态。

由于每个侦听站在传输的帧中看到的持续时间值相同，因此它们都可能在这段时间过去后

决定传输自己的帧，这可能导致冲突。所以，在实际中，除持续定时器外，每个无线工作站还必须实现一个随机后退定时器，传输帧之前，工作站必须选择一个要等待的随机时隙数，这个数字位于 0 和最大争用窗口值之间。这里的基本思想是，准备传输的工作站必须等待一段随机时间，以减少试图立即传输的工作站数量。

这个过程被称为分布式协调功能（Distributed Coordination Function，DCF），图 1-2 对其进行了说明。三位无线用户都有一个帧需要发送，它们所需的时间各不相同，发生的情况如下所述。

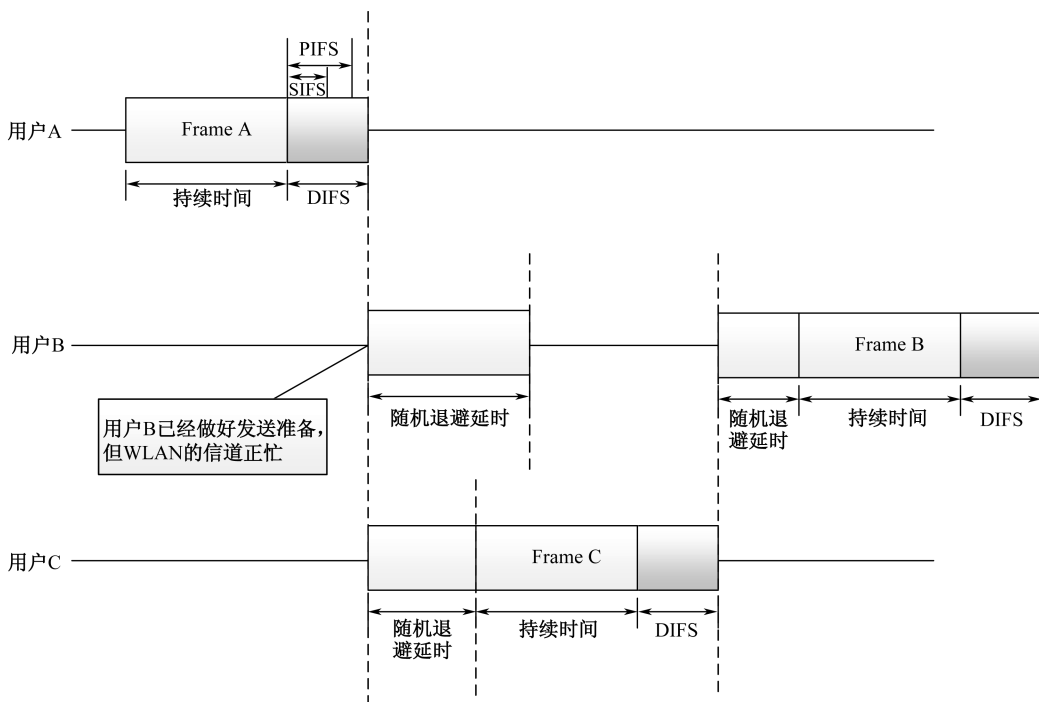


图 1-2　使用 DCF 过程避免冲突

① 用户 A 侦听并确定没有其他用户在传输，因此传输自己的帧并通告持续时间。

② 用户 B 有一个帧需要传输，他必须等待用户 A 的帧传输完毕，再等待 DIFS 时间过去。

③ 用户 B 在传输前等待一段随机退避时间。

④ 在用户 B 等待期间，用户 C 有一个帧需要传输，他通过侦听发现没有人在传输，用户 C 等待一段随机时间，但比用户 B 的随机时间短。

⑤ 用户 C 传输一个帧，并通告其持续时间。

⑥ 用户 B 传输前必须等待该持续时间加上 DIFS 时间。

由于后退定时器是随机的，多台工作站仍可能选择相同的退避时间，因此无法防止这些工作站同时传输数据，进而导致冲突。这样，在无线网络中将会出现传输错误，而接收站不会返回确认，为此发送站必须考虑重新发送其帧。

最后，工作站在其随机后退定时器过期后并准备传输数据时，如果发现有人正在传输，该如何办呢？它必须再等待当前正在传输的帧的持续时间加上 DIFS 时间和随机后退时间。

1.1.2　WLAN 的组成部分

从最底层说，无线介质没有固定的组织结构，例如，具有无线功能的计算机可以随时随地启动其无线适配器并与其他设备进行通信。

在 IEEE 802.11 中，一组无线设备被称为服务集（Service Set）。这些设备的服务集标识符（SSID）必须相同，服务集标识符是一个文本字符串，长度为 1～32 字节，包含在发送的每帧中，如果发送方和接收方的 SSID 相同，这两台设备将能够通信。作为最终用户工作站，计算机为无线网络的客户端，它必须有无线网络适配器和支持程序（同无线协议交互的软件）。

IEEE 802.11 标准让多个无线客户端能够彼此直接通信，而无须其他网络连接方式，这被称为对等无线网络（Ad Hoc）或独立基本服务集（Independent Basic Service Set，IBSS），如图 1-3（a）所示。

对可通过无线介质进行传输和接收帧的设备数量没有限制，一个无线工作站能否接收来自其他工作站的数据以及向它们发送数据取决于很多因素，这使得人们难以为所有的工作站提供可靠的无线接入。

IEEE 802.11 基本服务集（BSS）包含一个接入点（AP），它充当该服务集的集线器，负责集中控制一组无线设备的接入，要使用无线网络的无线客户端都必须向 AP 申请成员资格，AP 要求客户端满足下述条件才允许其加入：

① 匹配的 SSID；

② 兼容的无线速率；

③ 身份验证凭证。

向 AP 申请成员资格被称为关联（Association），客户端必须发送一条关联请求消息，AP 通过发送关联应答消息来批准或拒绝请求。关联后，前往和来自该客户端的数据都必须经过 AP，如图 1-3（b）所示。客户端之间不能像对等网络或 IBSS 那样直接通信。

无论关联状态如何，任何计算机都能够侦听和接收通过无线介质传输的帧，在无线电波的覆盖范围内，任何人都可以接收通过它们传输的帧。

然而，无线 AP 并不像以太网集线器那样属于被动设备，AP 负责管理其无线网络，通告自己的存在让客户端能够与之关联，并控制通信过程。例如，前面介绍过，通过无线介质成功发送（没有发生冲突）的每个数据帧都必须得到确认，AP 负责将确认帧发回给发送工作站。

> **注意**
>
> 一个 BSS 只包含一个 AP，并且没有连接到常规以太网，在这种设置中，AP 及其关联的客户端组成一个独立的网络。

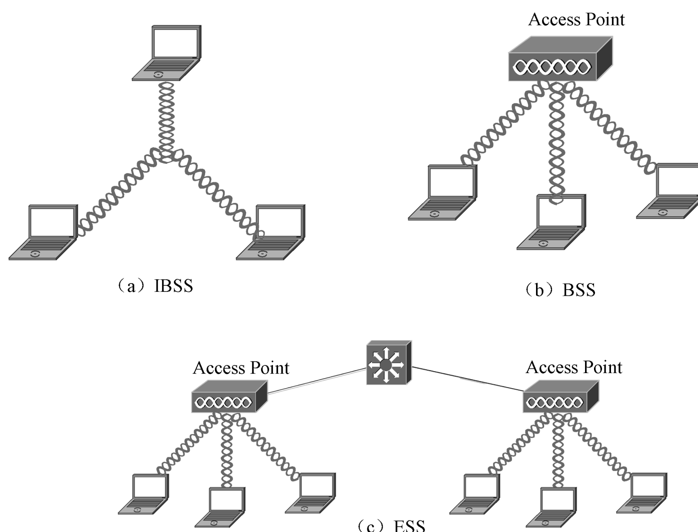


图 1-3　无线服务集的组成

AP 也可以连接到以太网，因为它同时具备无线和有线功能。对于位于不同地方的 AP，可以通过交换型基础设施将它们连接起来，这被称为 IEEE 802.11 扩展服务集（ESS），如图 1-3（c）所示。

在 ESS 中，无线客户端可同其附近的 AP 相关联，如果该客户端移到其他地方，可同另一个位于附近的 AP 相关联。IEEE 802.11 标准还定义了一种支持客户端漫游（当客户端移动时，可调整其关联的 AP）的方法。

1.1.3　接入点的工作原理

AP 的主要功能是将无线数据桥接到常规有线网络中，AP 能够接受来自大量无线客户端的连接请求，让它们成为 LAN 的一员，就像这些客户端使用的是有线连接一样。

AP 还可以用作网桥，在两个相隔较远的局域网之间建立一条无线链路，在这种情况下，无线链路的两端都需要一个 AP，AP 到 AP（视线可达）链路常用于连接办公大楼或城市。

Cisco 开发了一种 AP 平台（无线网状网络），能够以菊花链或网状网的方式在 AP 之间传输数据流，这让无线局域网能够覆盖更大的户外开阔区域，而不需要使用网络线缆。AP 之间组成一个全互连拓扑，就像 AP 之间通过无线连接互连的 ESS。

AP 充当中央接入点（名称 AP 由此而来），负责控制客户端对无线局域网的访问，客户端要使用 WLAN，必须首先同 AP 建立关联，AP 允许随便接入（任何客户端可与之关联），也可以严格控制接入，允许关联前要求提供认证凭证或满足其他条件。

WLAN 的工作原理与来自无线连接远端的反馈密切相关，例如，在关联和使用 WLAN 之

前，客户端必须同 AP 握手，这确保无线连接是双向和正常运行的，因为客户端和 AP 必须能够成功地发送和接收帧，这消除了单向通信（客户端能够侦听到 AP，但 AP 无法侦听到客户端）的可能性。另外，AP 还能够要求客户端满足某些条件才允许其关联，从而控制其 WLAN 的众多方面，例如，AP 可以要求客户端在关联期间支持特定的速率、特定的安全措施和特定的凭证。

可以将 AP 视为转换网桥，在第二层对来自不同介质的帧进行转换和桥接，简单地说，AP 负责将 VLAN 映射到 SSID。图 1-4 的左半部分说明了一点。在这里，位于有线网络中的 VLAN10 通过一个处于接入模式的交换机端口扩展到了 AP，该 AP 将 VLAN10 映射到一个 SSID 为 Marketing 的无线局域网，SSID 为 Marketing 的用户将属于 VLAN10。

可以将这种概念进行扩展，以便能够将多个 VLAN 映射到多个 SSID。为此，AP 必须通过一条为多个 VLAN 传输数据的中继链路（Trunk）连接到交换机。在图 1-4 的右半部分，VLAN10 和 VLAN20 都通过中继链路连接到 AP。AP 根据 IEEE 802.1q 标记将不同的 VLAN 映射到不同的 SSID，例如，VLAN10 被映射到 SSID Marketing，而 VLAN20 被映射到 SSID Engineering。

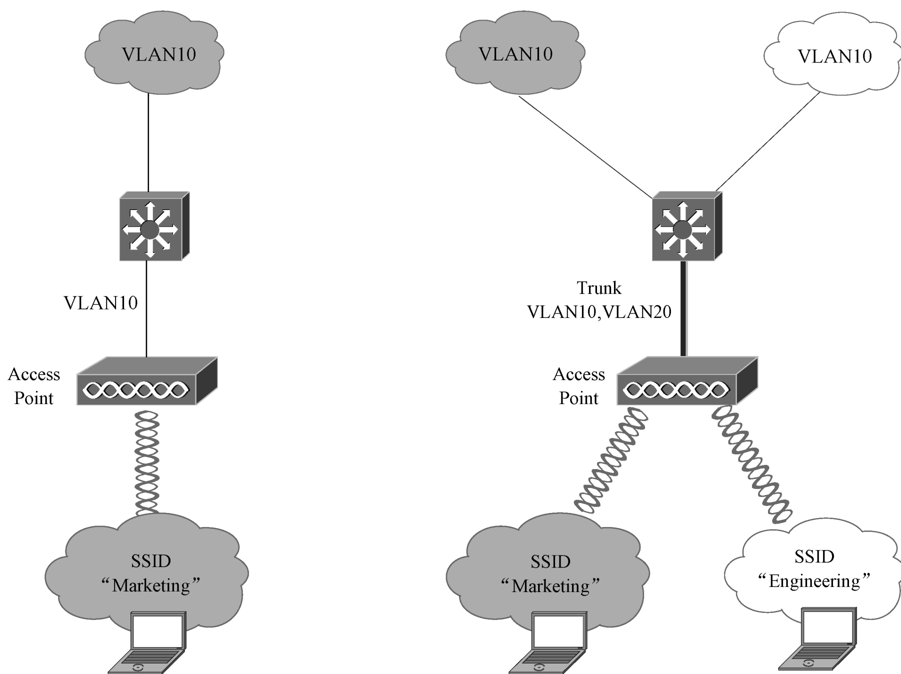


图 1-4　VLAN 和 SSID 的映射

实际上，当 AP 使用多个 SSID 时，它通过无线介质将 VLAN 连接到最终用户，最终用户必须使用合适的 SSID，而 SSID 又被映射到相应的 VLAN。

1.1.4 无线局域网蜂窝

AP 为其覆盖范围内的客户端提供 WLAN 连接性，信号的覆盖范围取决于 AP 的天线辐射图。在户外，这可能是环绕全向天线的一个圆，至少在透视上是一个圆。辐射图是三维的。在多层大楼中，也将覆盖上面和下面的楼层。

必须仔细规划 AP 的位置，使其覆盖范围与所需的范围匹配，即使根据楼层平面图或户外布局来确定 AP 的位置，WLAN 也将在不断变换的条件下运行，虽然 AP 的位置是固定的，但无线客户端将频繁地变换位置。

为确定 AP 的位置和覆盖范围，最好的方法是进行现场勘查（Site Survey），将 AP 放在所需的位置，让客户端不断移动，并实时测量信号的强度和质量。这里的理念是，在实际环境中测试 AP 的覆盖范围，其中有可能干扰客户端连接的障碍物。障碍物及其对 RF 信号的影响将在本章后面的内容中介绍。

AP 的覆盖区域被称为蜂窝（Cell），位于该蜂窝内的客户端能够同 AP 关联，并使用无线局域网。图 1-5 说明了这种概念，其中有一个客户端位于蜂窝外，因为它不在 AP 的信号覆盖范围内。

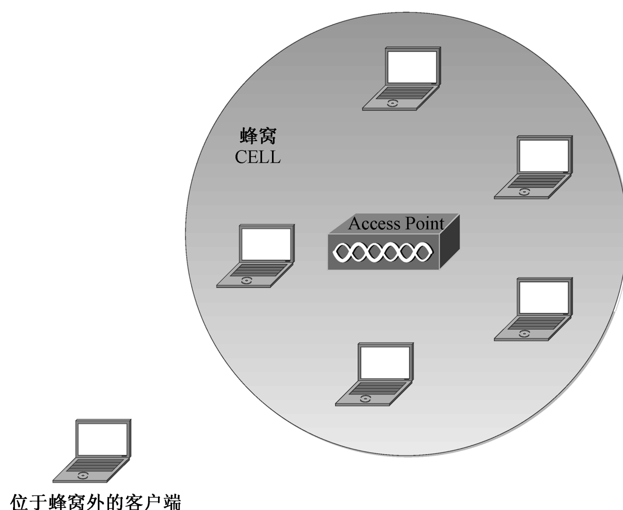


图 1-5 位于蜂窝内的客户端

假设一个典型的室内 AP 蜂窝的半径为 100 英尺（1 英尺=30.48 厘米），能够覆盖多个房间或走廊的一部分，客户端可以在该蜂窝内移动，并在任何地方使用 WLAN。然而，该蜂窝的局限性非常强，因为客户端可能需要移到周围的房间或楼层，而不希望失去网络连接。

为扩大 WLAN 的覆盖范围，可在周围安装其他 AP，从而添加更多的蜂窝。这里的理念是，通过增加 AP，使用蜂窝覆盖客户端可能移动到的所有区域。实际上，蜂窝之间应该有一定程

度的重叠，如图 1-6 所示。

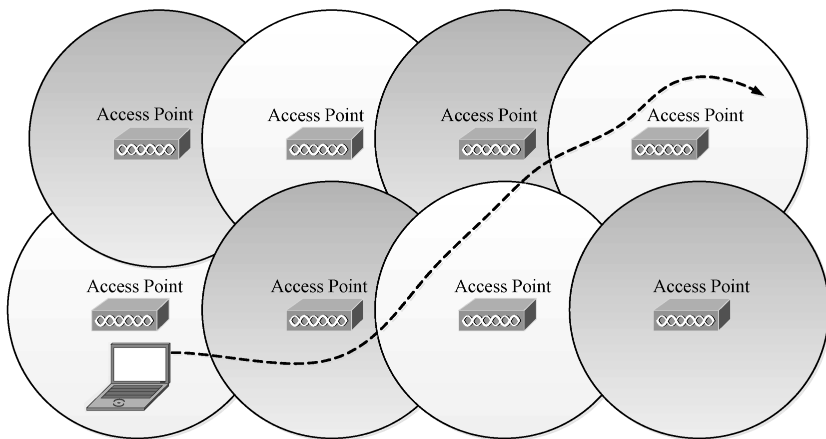


图 1-6　通过排列蜂窝实现无缝覆盖

如果 AP 蜂窝发生重叠，相邻的 AP 将不能使用相同的频率。如果两个相邻的 AP 使用相同的频率，将相互干扰。在整个覆盖区域，AP 的频率应交替变化。这种概念将在下面的章节更详细地介绍。

客户端同一个 AP 关联后，便可以自由移动，客户端从一个 AP 蜂窝移动到另一个 AP 蜂窝后，将同另一个 AP 关联。客户从一个 AP 移动到另一个 AP 被称为漫游，图 1-6 说明了这种移动：当笔记本电脑沿图中所示的路径移动时，将穿越多个 AP 蜂窝。

客户端从一个 AP 蜂窝移动到另一个 AP 蜂窝内后，必须同新的 AP 建立关联。另外，在发生漫游前，客户端发送的数据也将从原来的 AP 中继到新的 AP。这样，每个客户端在任何时刻都只通过一个 AP 连接到 WLAN，最大限度地降低了漫游期间发送或接收的数据丢失的可能性。

在设计无线局域网时，你可能试图将每个 AP 覆盖尽可能大的区域，并让每个 AP 以最大的发射功率运行，以充分利用其覆盖范围，这样做还可以减少所需的 AP 数，进而降低整体成本。然而，应考虑其他一些因素，例如，当将 AP 配置为提供较大的覆盖范围时，也为过度拥挤打开了大门。AP 蜂窝实际上是一种半双工共享介质，所有的客户端将共享它，随着客户端数量的增多，每个客户端可用的宽带和可传输时间将减少。相反，应考虑缩小蜂窝（通过降低发射功率），使得只有离 AP 较近的客户端才能与之相关联并使用其提供的宽带。AP 还可控制在给定时刻关联的客户端数量，这对于对时间敏感或带宽密集型数据流（如语音、视频和医疗应用程序）来说非常重要。

被缩小的蜂窝常被称为微蜂窝，在需要严格控制的环境中（如股票交易所），可进一步扩展这种概念，在这种环境中，将最大限度地缩小 AP 的功率和蜂窝，此时蜂窝被称为微微蜂窝（Pico Cell）。

1.2 无线射频简介

射频传输的接收是 WLAN 的有机组成部分，我们应该理解射频（RF）的基本理论，以便能够高效地设计和诊断 WLAN 网络。然而，RF 理论涉及复杂的数学和物理原理，本节从实用的角度介绍 RF，不涉及任何方程式。

1.2.1 RF 的工作原理

在射频（RF）通信中，一台设备发送振动信号，并由一台或多台设备接收，这种振动信号基于一个常数，被称为频率。发送方使用固定的频率，接收方可以调到相同的频率，以便接收该信号，我们在汽车中调收音机时就有这方面的经验。

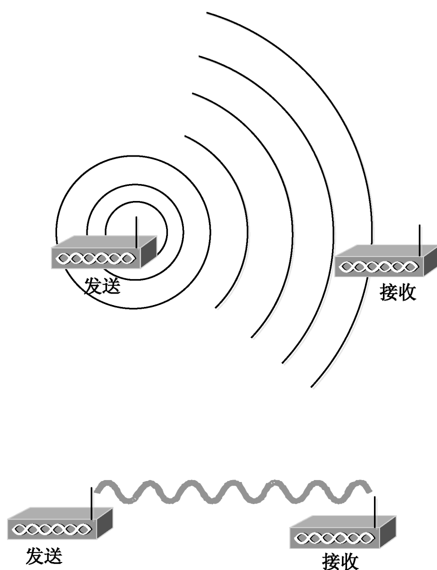


图 1-7 无线信号

发送站有生成 RF 信号的发射器、天线以及连接两者的电缆；接收站与此相同，但通过天线和电缆接收信号。出于简化的目的，假设无线工作站使用的天线非常小，并且在所有方向均匀地发送或接收 RF 信号，如图 1-7 的上半部分所示。其中的每个弧表示发射器生成的无线电波的一部分，每个弧实际上是一个球，因为无线电波是在三维空间移动的，这也可以显示为表示 RF 信号的振动波，如图 1-7 的下半部分所示。虽然该示意图从技术上说不正确，但这里旨在说明 RF 信号是如何在两台设备之间传输的。

用于类似功能的频率范围称为波段。例如，调幅无线波段的频率范围为 550～1 720 MHz。有些无线局域网通信使用的是 2.4 GHz 的波段，而其他无线局域网使用的波段为 5 GHz。在这里，波段是使用大概的频率表示的，2.4 GHz 实际上表示的是频率范围 2.412～2.484 GHz；而 5 GHz 实际上指的是频率范围 5.150～5.825 GHz。

无线工作站发送的信号被称为载波信号，以频率 840 MHz 进行广播的广播站的载波在 840 MHz 处振动。如果仅接收到载波信号，将无法从中提取任何内容，载波信号只是一种频率固定的稳定信号，载波信号本身不包含任何音频、视频或数据，因为它只用于承载其他信号。

要发送其他信息，发射器必须对载波信号进行调制，以独特的方式插入信息（对其进行编码），接收站必须进行相反的处理，对信号进行解调以恢复原始信息。

有些调制技术很简单——调幅（AM）广播采用调幅技术，即根据音频信息改变载波信号的强度。FM 广播采用调频技术（FM），即音频的高低导致载波信号的频率发生变化。WLAN 使用的调制技术要复杂得多，因为它们的速率比音频信号高得多，WLAN 调制的理念是在无线信号中封装尽可能多的数据，并尽可能减少由于干扰或噪声而丢失的数据量。由于数据丢失后必须重传，同此会占用更多的无线资源。

调制方案通常会导致载波信号有轻微的变化，因此发送方和接收方期望载波的频率是固定的，并在特定的范围内变化，这种范围称为信道（Channel）。信道通常用数字或索引（而不是频率）表示。WLAN 信道是由当前使用的 IEEE 802.11 标准决定的。图 1-8 说明了载波频率（中间频率）、调制、信道和波段之间的关系。

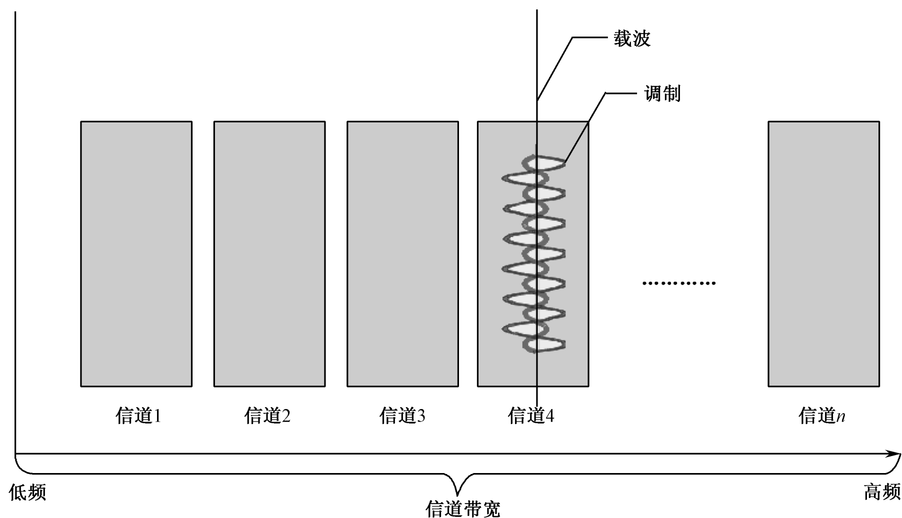


图 1-8 RF 信号术语

1.2.2 RF 的特征

RF 信号以电磁波的方式通过空气传播，在理想情况下，信号到达接收方时与发送方发送的相同，而实际上并非总是如此。当 RF 信号从发送方传输到接收方时，将受其遇到的物体和材质的影响，本节将简要地探讨影响无线信号传播的条件。

1．反射

无线信号以电波的方式在空中传播时，如果遇到密集的反射材质，将发生反射，以电灯发出的光线为例，虽然大多数光线从电灯出发向各个方向传播，但有些可能在碰到房间中的物体后发生反射，反射光回到电灯，或者照射到房间的其他区域，使区域更亮。

图 1-9 说明了 RF 信号的反射。室内的物体，如金属家具、文件柜和金属门等可能导致反射，室外的无线信号可能在遇到水面或大气层时发生反射。

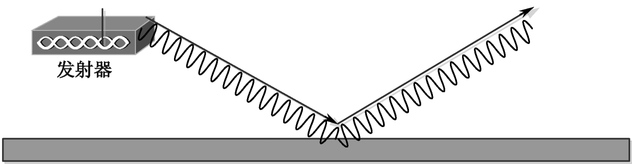


图 1-9　RF 信号的反射

2．折射

在两种密度不同的介质之间的边界上，RF 信号也可能发生折射。反射是遇到表面后弹回来，而折射是在穿过表面时发生弯曲。折射信号的角度与原始信号不同，传播速度也可能降低，图 1-10 说明了这种概念。例如，信号在穿过密度不同的大气层或建筑物墙面时，将发生折射。

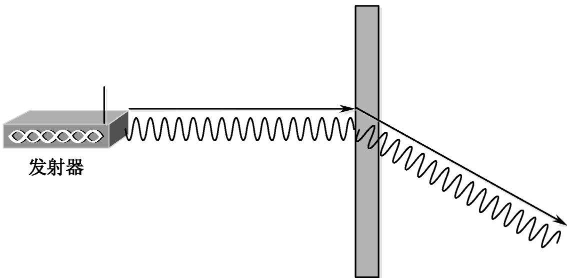


图 1-10　RF 信号的折射

3．吸收

当 RF 信号进入能够吸收其能量的材质时，信号将衰减。材质的密度越高，信号的衰减越严重，图 1-11 说明了吸收对信号的影响，过低的信号强度将影响接收方收到的信号，最常见的吸收情形是，无线信号穿过水分，水分可能包含在无线传输路径中的树叶或无线设备附近的人体中。

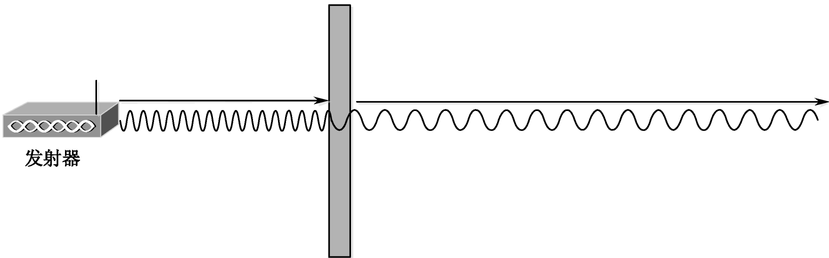


图 1-11　RF 信号的吸收

4．散射

当 RF 信号遇到粗糙、不均匀的材质或由非常小的颗粒组成的材质时，可能向很多不同的方向散射。这是因为材质中不规则的细微表面将反射信号，如图 1-12 所示。无线信号穿过充满灰尘或沙粒的环境时将发生散射。

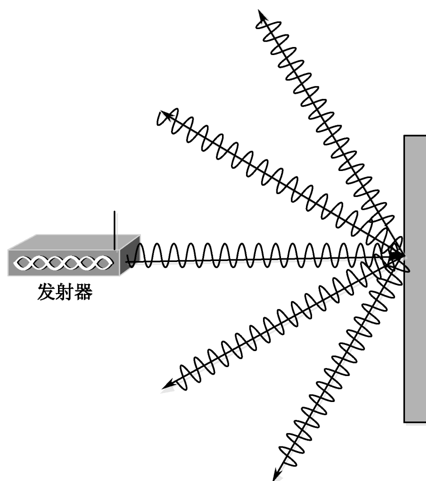


图 1-12　RF 信号的散射

5．衍射

假设 RF 信号遇到其不能穿过的物体或能够吸收其能量的物体，读者可能认为将出现一个“阴影”（其中没有信号），就像光照射在物体上时会导致阴影一样。如果形成这样的阴影，将导致 RF 信号没有覆盖的静区，然而，在 RF 传播中，信号通常会通过弯曲绕过物体，最终组合成完整的电波。

图 1-13 说明了不透明物体（阻断或吸收 RF 信号的物体）将导致 RF 信号发生衍射。衍射生成的是同心波而不是振动信号，因此将影响实际电波。在该图中，衍射导致信号能够绕过吸收它的物体，并完成自我修复，这种特殊性使得在发送方和接收方之间有建筑物时，仍能够接收到信号，然而，信号不再与原来的相同，它因为衍射而失真。

6．菲涅耳区

如果物体是悬空的，平行于地面传播的 RF 信号将绕过物体的上、下两端发生衍射，因此信号通常能够覆盖物体的“阴影”。然而，如果非悬空物体（如建筑物或山脉）阻断了信号，在垂直方向信号将受到负面影响。

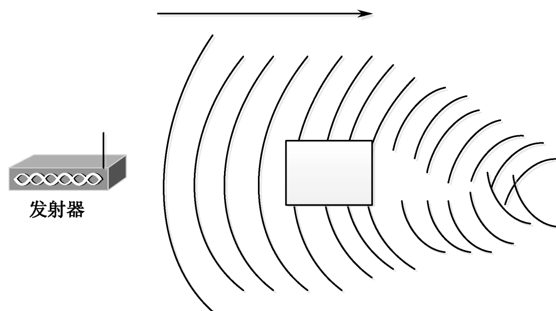


图 1-13　RF 信号的衍射

在图 1-14 中，一座大楼阻断了信号的部分传输路径。由于在沿大楼前端和顶端发生衍射，信号发生弯曲和衰减，导致信号无法覆盖大楼后面的大部分区域。

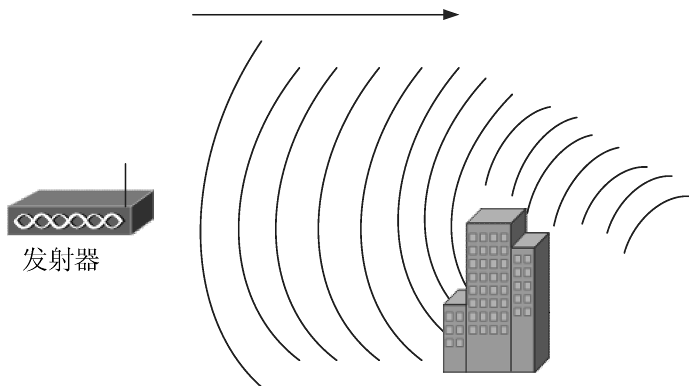


图 1-14　障碍物导致的信号衍射

在狭窄的视线（Line-of-sight）无线传输（这非常适合长距离传输）中，必须考虑到这种衍射，这种信号不沿所有方向传输，而是聚焦成束，如图 1-15 所示。要形成视线路径，在发送方和接收方的天线之间，信号不能受任何障碍物的影响。在大楼或城市之间的路径中，通常有其他大楼、树木或其他可能阻断信号的物体。在这种情况下，必须升高天线，使其高于障碍物，以获得没有障碍的路径。

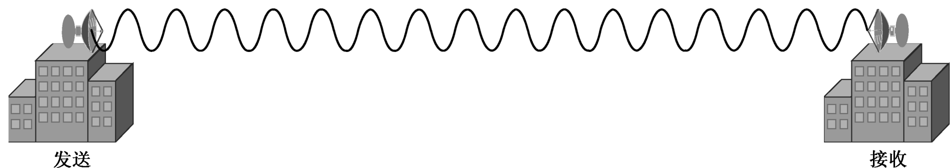


图 1-15　沿视线传输的无线信号

当进行远距离传输时，弯曲的地球表面也将成为影响信号的障碍物。当距离超过两英里时，

将无法看到远端，因为它稍低于地平线。尽管如此，无线信号通常沿环绕地球的大气层以相同的曲度传播，即使物体没有直接阻断信号，狭窄的视线信号也可能受衍射的影响。在环绕视线的椭球内也不能有障碍，这个区域被称为菲涅耳区，如图 1-16 所示。如果菲涅耳区内有物体，部分 RF 信号可能发生衍射，这部分信号将弯曲，导致延迟或改变，进而影响接收方收到的信号。

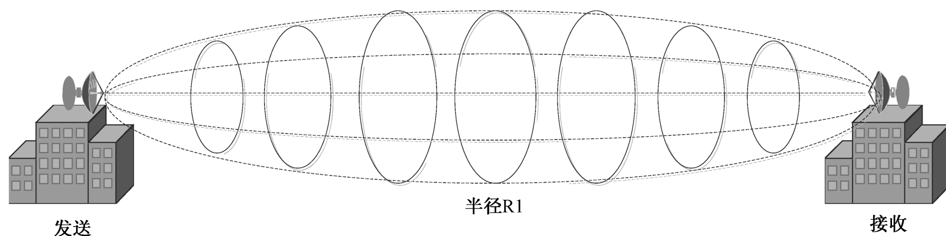


图 1-16　菲涅耳区

在传输路径的任何位置，都可以计算出菲涅耳区半径 R1。在实践中，物体必须离菲涅耳区的下边缘有一定的距离，有些资料建议为半径的 60%，其他资源则建议为 50%。

在图 1-17 中，在信号的传输路径中有一座大楼，但没有阻断信号束，然而，它却位于菲涅耳区内，因此信号将受到负面影响。

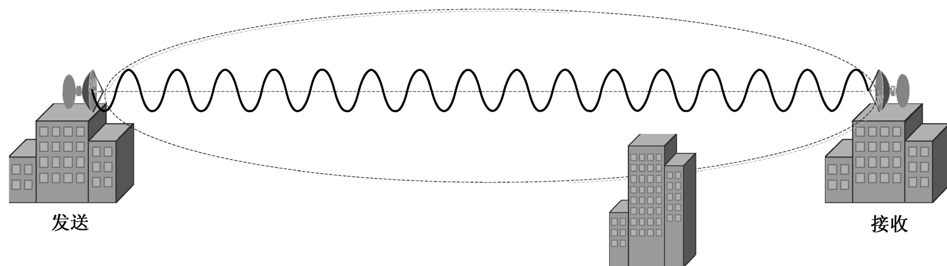


图 1-17　菲涅耳区内的障碍物导致信号质量降低

通常，应增加视线系统的高度，使菲涅耳区的下边缘比所有障碍物高，当传输路径非常长时，弯曲的地球表面将进入菲涅耳区并出现问题，如图 1-18 所示。

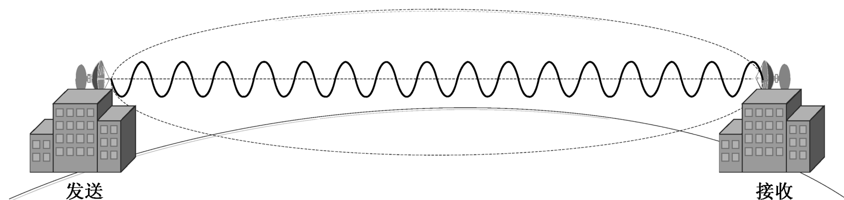


图 1-18　弯曲的地球表面进入了菲涅耳区

可以使用一个复杂的公式来计算菲涅耳区的半径。事实上，我们只需要知道存在菲涅耳区，并且其中不能有任何障碍物即可。表 1-1 列出了当使用频段为 2.4 GHz 时，无线传输路径中点处的菲涅耳区半径值。

表 1-1　菲涅耳区的半径

传输距离 / ml.	路径中点处的菲涅耳区的半径 / ft.
0.5	16
1.0	23
2.0	33
5.0	52
10.0	72

注释：1 ml.=1.609 km；1 ft.=30.48 cm

有关计算菲涅耳区的半径的更详细信息，请通过 www.wikipedia.org 查阅。百度网站提供了一个菲涅耳区的半径计算器，其网址为 http://wenku.baidu.com。

1.2.3　描述 RF 信号强度的术语

可使用单位为瓦（W）或毫瓦（mW）的功率或能量来度量 RF 信号的强度。为了让大家对信号功率有深入的认识，表 1-2 列出了各种信号源的典型输出功率。

表 1-2　典型 RF 输出功率

信号源	输出功率
短波广播站	500 000 W
AM 广播站	50 000 W
微波炉（2.4 GHz）	600～1 000 W
手机	200 mW
无线局域网	1～100 mW

功率的范围非常大，这使得比较和计算起来非常困难，分贝（dB）是一种更灵活的表示功率的方式，原因有两个：

- dB 度量的是实际功率和参考功率的比例；
- dB 是对数，能够以线性方式表示更大范围的值。

要计算以 dB 为单位的功率比例，可使用下面的公式：

$$1\text{dB}=10\lg(P_{sig}/P_{ref})$$

其中，P_{sig} 为实际信号功率，P_{ref} 为参考功率。最常用的参考功率为 1.0 mW 或 1.0 W。在

这种情况下，分贝的缩写将被修改为指出所用的参考功率。

- dBm：信号相对于 1 mW 的强度（dBm 中的 m 表示毫瓦）；
- dBw：信号相对于 1 W 的强度。

在无线局域网中，经常使用单位 dBm，因为它们使用的功率在 100 mW 左右。例如，假设一个无线 AP 的发射功率为 100 mW，则当使用分贝表示时，输出功率为 10lg（100 mW/ 1 mW 即 20 dBm。

如果输出功率降低到 1mW，结果将为 10lg（1 mW/1 mW），即 0 dBm。因此，0 dBm 表示输出功率与参考功率相同。到目前为止，这里讨论的 dB 值都为正，这表示实际功率比参考功率高。在大多数情况下，发射器的 dBm 值为正，因为它们的功率高于参考功率。dB 值也可以为负，这并不意味着功率为负，而意味着功率比参考功率低。例如，信号功率为 0.5 mW 时，dB 值将为 10lg（0.5 mW/ 1 mW），即−3 dBm。

在该示例中，功率 0.5 mW 为前一个示例中的功率 1.0 mW 的一半，而 dBm 值却从 0 变成了−3，这种变化幅度很重要，它说明了两个重要的经验规则：

- 功率每减少一半，dB 值将减小大约 3；
- 功率每增加一倍，dB 值将增大大约 3。

接收器的 dBm 值通常为负，因为接收器必须对低功率信号（功率比参考功率 1 mW 低得多）非常敏感，这样才能清晰地接收到非常弱的信号。接收器的功率被称为接收器的灵敏度。

1. 信号衰减

RF 信号离开发射器后（甚至在到达天线前），都将受外部因素的影响而降低强度，这被称为信号衰减。导致信号衰减的因素如下所述：

- 发射器和天线之间的电缆衰减；
- 信号在空中传输时的自由空间衰减；
- 外界的障碍物；
- 外部的噪声或干扰；
- 接收器和天线之间的电缆衰减。

这里列出了信号从发射器传输到接收器的过程中遇到的各种情况，衰减将不断累积，导致信号质量降低，端到端的总衰减称为路径衰减。

在室内无线局域网环境中，连接天线的电缆非常短，其带来的衰减可忽略不计。通常，天线内置在无线适配器或笔记本电脑中，或者直接连接到 AP 中的 RF 电子装置，主要的路径衰减是由房间或建筑物内的物体以及 AP 和无线客户端之间的距离引起的。

在室外环境中，可能存在上述各种因素引起的衰减。在视线无线路径中，AP 和天线之间的电缆可能非常长，如果仔细选择了路径，外部物体带来的衰减可能不大，而外部干扰可能是个大问题，附近可能有无线装置，在信道的使用上可能发生冲突，天线也可能没有对准。

在任何环境中，自由空间衰减都很大，RF 信号的功率与传输距离的平方呈反比，这意味

着随着接收器远离发射器，接收的信号强度将急剧降低。

例如，表 1-3 说明了 dB 值随距离的增大而降低的程度，其中列出的 dBm 值是相对的。注意：距离每增加 10 倍，信号强度将降低 20 dBm；当距离增大 100 倍时，信号强度将降低 40 dBm。

表 1-3　距离导致的相对信号衰减

距离 / m	信号功率 / mW	相对强度 / dBm
1	100	+20
5	4.0	+6
10	1.0	0
25	0.16	−8
50	0.04	−14
100	0.01	−20

接收器可能离发射器太远，无法收到能够识别的信号，也可能是它们之间有很多吸收或扭曲信号的物体。例如，即使是普通的建筑材料，如干饰面内墙、砖墙或水泥墙、木质或金属门、门框和窗户，都会导致信号衰减。有一些人估计，在办公环境中，当离 AP 100 m 时，无线信号的衰减为 100 dBm。因此，在实际环境中必须使用 WLAN 信号进行现场勘察。

2．信号增益

在传输路径中，AP 信号也可能受增加其强度的因素影响，信号增益是由下列因素导致的。

- 发送方的天线增益；
- 接收方的天线增益。

天线本身并不能提高信号的功率，那它如何实现增益呢?首先来看发送方的天线，其增益指的是天线接收 RF 信号以及将其沿特定方向发射出去的能力。

然而，天线可以有不同的方向（辐射图）。那么，一种天线是否优于另一种天线取决于它聚焦信号的方向吗？不一定。通常，如果天线能够将 RF 能量聚焦到更窄的范围内，其增益就更高。因此，增益较高的天线通常能够将信号传输更远的距离。

天线增益指的是其聚焦信号能量的能力，这是相对于根本不聚焦能量的天线而言的，各向同性天线就是一种根本不聚焦的天线，其理论模型为一个点。它以相同的方式沿各个方向传播信号，辐射图为球形。它不能聚焦 RF 能量，可用于标准比较。

天线增益通常使用单位 dBi，其计算方法与 dBm 相同，唯一的差别是，参考功率为各项同性天线发射的信号功率（其中的 i 因此而来）。

3．无线路径的性能

经常会在 AP 看到其发射功率标称，这通常指的是发射器的输出功率，没有考虑天线和电

缆的影响，实际发射的信号的功率取决于使用的天线类型和天线电缆的长度。

一种更真实的标称是各向同性高效辐射功率（Effective Isotropic Radiated Power , EIRP），EIRP 的计算方法是，将发射器功率（单位为 dBm）加上发射天线的增益（单位为 dBi），再减去电缆衰减（单位为 dB）。

例如，使用衰减为 3 dB 的电缆将功率为 100 mW（20 dBm）的发射器连接到增益为 16 dBi 的天线上，该发射系统的 EIRP 为 20 dBm+16 dBi–3 dB=33 dBm。在设计完整的无线系统时，不能仅仅考虑发射器或 AP 的功率，还需要考虑整个无线链路中将导致增益或衰减的每个组件，为确定路径性能或总体增益，最简单的方法是将所有的增益或衰减 dB 值相加。作为一种经验规律，可使用下面的公式：

系统增益 = 发射功率（dBm）
+发射天线的增益（dBi）
+接收天线的增益（dBi）
–发射端的电缆衰减（dB）
–接收端的电缆衰减（dB）
–接收器的灵敏度（dB）

注意，这里将接收器的灵敏度视为衰减，因此将其减去。接收器的灵敏度指的是可用信号的最低功率，因此必须减去它，以得到最终的增益。无线链路的最大长度取决于整体路径性能。当总路径衰减等于或大于且路径增益时，接收器将无法收到信号。

1.2.4　WLAN 天线

可在无线局域网中使用的天线有很多，每种天线都有特定的用途，这取决于其覆盖范围（辐射图）或给信号带来的增益。

1．全向天线

全向天线（如图 1-19 所示的天线）可制作为圆柱形。图 1-19 中所示的橡皮条式天线可根据 AP 的安装方式进行折叠。另一种全向天线是偶极天线，它也呈细圆柱体状，很多型号的 AP 都内置了这种天线。

全向天线通常在同一个平面的各个方向上均匀地传播信号，但在天线所在的方向上并非如此，因此辐射图为圆环形，如图 1-19 的右半部分所示，这种天线非常适合用于大房间或整个楼层，在这种环境下，将 AP 或其天线放在中央。

由于全向天线在广阔的区域内分配 RF 能量，因此其增益较低，大约为 2 dBi。

有时候，RF 信号将由于反射、折射或衍射而失真。当受影响的信号和原始信号一起到达接收器后，两个信号通常会彼此抵消。因此，接收器收到的信号强度将急剧降低，甚至收不到信号。当信号同其采取不同路径的拷贝相互竞争时，将导致多路干扰（Multipath Interference）。

为解决这种问题，只需稍微移动接收器的天线（大约半个波长的距离），便可以接收到质量更好的信号。很多 AP 都默认有两根全向天线，这些天线相隔的距离很合适，使得其中有一个天线能够收到质量最好的信号。同时使用两根天线被称为分集（Diversity）。

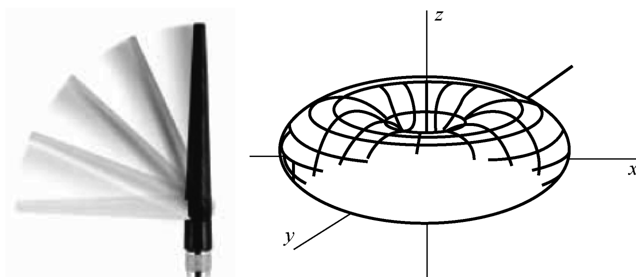


图 1-19　一种全向天线及其辐射图

2．半定向天线

半定向天线有一个细长的区域，非常适合用于覆盖长走廊上的很多房间，在这种环境中，天线安装在区域的一端。它们还可用于覆盖室外区域，安装在墙面上的板状天线呈扁平的矩形状，以方便安装在走廊端的墙面上。板状天线的辐射图呈鸡蛋状，其中的一端为墙面，这种天线的增益为 6～8 dBi。

如图 1-20 所示的 Yagi 天线呈细圆柱状，内部有多个平行的元件组成。其辐射图呈鸡蛋状，并沿天线的两端向外延伸。注意：在这种天线的后面几乎没有信号，这不同于全向天线。Yagi 天线的增益大约为 10～14 dBi。

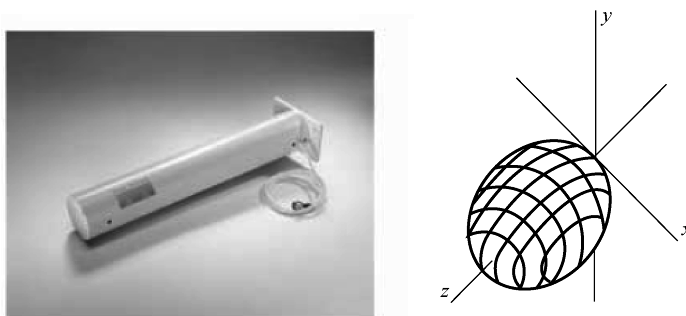


图 1-20　半定向天线及其辐射图

3．高度定向的天线

在视线无线路径中，RF 信号必须沿狭窄的信号束传播很长的距离，高度定向的天线是专门为此设计的，它将 RF 能量聚焦到一个狭长的椭圆形区域内。由于目标是一个接收器的位置，

因此天线无须覆盖视线之外的其他区域，这种天线非常适合用于建立大楼到大楼或场点到场点的链路，两个 AP 或天线相隔很远的情况。

如图 1-21 所示的碟形天线使用呈抛物面状的盘碟将收到的信号聚焦到中央的天线上。这种天线的辐射图长而窄，从盘碟向外延伸出去。这种聚焦辐射使得天线的增益大于 22 dBi，这在所有无线局域网天线中是最高的。

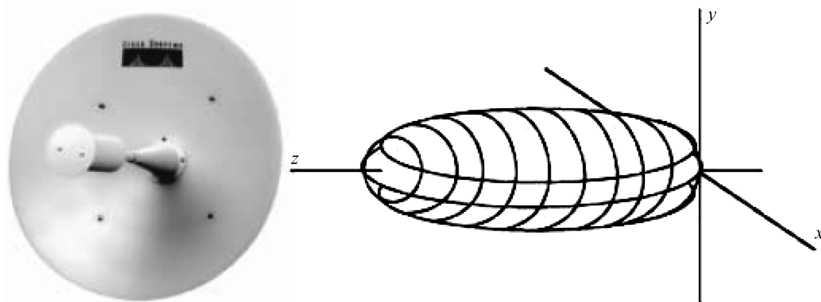


图 1-21　高度定向的碟形天线及其辐射图

1.3　WLAN 标准

所有的无线局域网标准都属于 IEEE 802.11 系列，每台无线设备都必须遵循其中一个或多个标准，这样才能同其他无线设备交互。

IEEE 802.11 标准定义了无线局域网在第一层和第二层的工作方式，这包括无线频率和信道，以及吞吐量、安全性和移动性。接下来将介绍几个基本标准。

1.3.1　管理机构

无线局域网频段无须许可就可使用，这使得任何人都可以使用它们，而无须申请使用牌照。然而，有多个机构对其进行管制，它们制定了有关可以使用哪些频率及信号功率的规则。

例如，在美国，联邦通信委员会（FCC，网址为 http://www.fcc.gov）负责管制无线频率的使用。其他机构负责制定全世界都必须遵守的无线标准，这包括制定了 IEEE 802.11 标准的电气和电子工程师协会（IEEE，网址为 http://www.ieee.org）和欧洲通信标准协会（ETSI，网址为 http://www.etsi.org）

在中国，工业和信息化部无线电管理局（网址为 http://www.srrc.org.cn）负责管制无线频率的使用。所有无线设备必须通过工业和信息化部无线电管理局的测试后获取入网许可证才能在中国销售，各个厂商无线设备入网核准证的详情可以到下面的网址查询：http://www.srrc.org.cn/others/WP_Search.aspx。

还有一些组织致力于为无线开发人员和用户提供有帮助的信息。WiFi 联盟（http://www.wi-fi.com）致力于测试不同厂商和平台之间的互操作性，其前身为无线以太网兼容性联盟（WECA）。无线设备通过 WiFi 联盟的认证意味着可以更好地支持 IEEE 802.11 协议。

WLAN 协会（WLANA，网址为 http://www.wlana.org）是一个非盈利的教育行业协会，致力于提供有关无线局域网及其公共应用的信息。

1.3.2 WLAN 帧类型和长度

遵循 IEEE 802.11 标准的设备必须使用特定类型的帧在 WLAN 中进行通信，有些帧由无线客户端使用，而其他帧只能供 AP 使用。

我们应熟悉下述几种帧。

① 管理帧用于管理 WLAN 通告和客户端成员资格，这包括下面几种类型的帧。

- 通告 AP 及其 WLAN 参数的信标；
- 客户端关联、重新关联和解除关联；
- 客户端认证和撤销认证。

② 控制帧用于控制客户端同 AP 的关联，包括下面几种类型的帧。

- 探测请求和响应，用于客户请求有关 AP 的信息时；
- RTS 和 CTS 消息，用于 AP 必须代表客户端通告帧持续时间时；
- 数据帧——由任何无线设备发送，包含数据或有效负载信息。

WLAN 帧包含长 32 字节的帧头和长 4 字节的帧校验序列（FCS）。帧中包含的源地址和目标地址是 48 位的 MAC 地址，就像 IEEE 802.3 以太网帧一样。

在发送的管理帧中，总是包含一个 48 位的基本服务集标识符（Basic Service Set Identifier，BSSID）字段。前面介绍过，BSS 必须包含一个 AP，它充当中央集线器，与所有客户端相连，BSSID 是该 AP 的 MAC 地址，它唯一地标识 AP 服务的一组设备。

1.3.3 IEEE 802.11b

标准 IEEE 802.11b 规定 WLAN 使用频段 2.4 GHz（2.4～2.5 GHz），而 FCC 只允许 WLAN 使用频率范围 2.4000～2.4835 GHz。

有趣的是，FCC 认为频段 2 .4 GHz 的主要用户是诸如微波炉等设备，其次才是 WLAN 设备，必要时总是让主要用户优先，您可能有过这样的经历，有人在做爆米花时，你办公室内的 WLAN 无法使用。

2.4 GHz 频段被称为工业、科学和医疗（ISM）频段，它包含 14 个信道，每个信道的宽度为 22 MHz，无线 AP 和客户如何隔离信道呢？

1．IEEE 802.11b 的信道

IEEE 802.11b 标准定义了一个频谱屏蔽器，即用于根据中间频率过滤出单个信道的模板。如图 1-22 所示，在中点两边的 11 MHz 处，信号必须衰减到–30 dBm，这形成了一个宽 22 MHz 的信道。信号可以进一步覆盖更大的频率范围，但在中点两边的 22 MHz 处，必须衰减到–50 dBm。

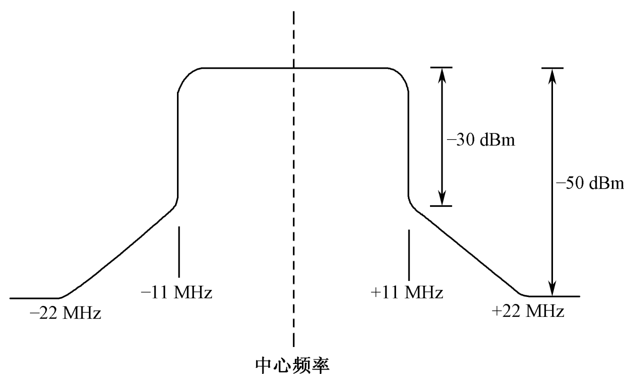


图 1-22 IEEE 802.11b 信道频谱屏蔽器

注意，整个频段覆盖的范围为 2.4000～2.4835 GHz，其宽度为 0.0835 GHz（83.5 MHz），这只能容纳大约 3.8（83.5/22）个完整的信道，又如何能提供 14 个信道呢？信道中心之间的间隔实际上为 5 MHz，而不是读者认为的 22 MHz，这导致信道之间几乎是完全重叠的，如果两个无线工作站使用相邻的信道，将会出现这样的问题：它们的信号渗透到对方的信道中，导致两个信道都受到破坏。解决方案是：使用尽可能多的彼此不重叠的信道，这使得只有信道 1、信道 6 和信道 11 可用，如图 1-23 所示。

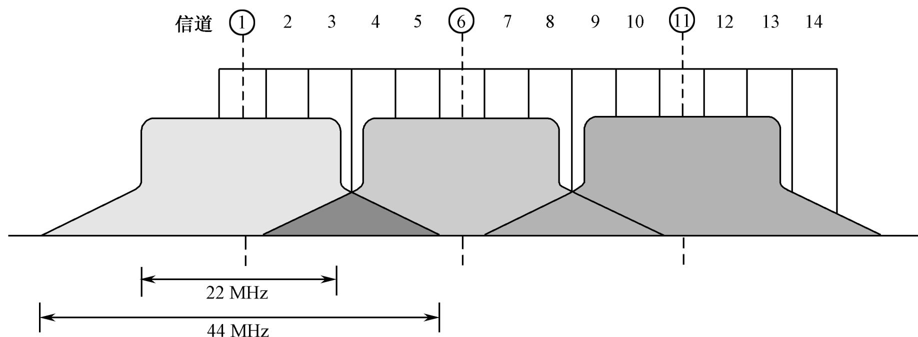


图 1-23 三个彼此不重叠的信道：信道 1、信道 6 和信道 11

2．IEEE 802. 11 b 的速率

遵循 IEEE 802.11b 标准的设计通常使用直接序列扩频（Direct Sequence Spread Spectrum,

DSSS）调制。信道的速率取决于客户端的功能和状态，然而，只支持速率 1 Mbps、2 Mbps、5.5 Mbps 和 11 Mbps，无线客户端和 AP 必须就支持的速率达成一致，客户端才能关联到 AP。

为何能支持不同的速率呢？这主要是 IEEE 802.11b 不断演进的结果。它最初只支持 1 Mbps 的速率，然后不断发展，支持的速率在不断提高。很显然，我们可能认为无线设备应该始终以最高的速率运行，以获得最高的吞吐量。

支持不同速率带来的副作用之一是，仅当离 AP 很近时才能成功地获得较高的速率，较高的速率使用的调制比较低的速率复杂，这要求信号质量更高，而这仅当离 AP 更近时才可能。随着客户端远离 AP，信号强度将降低，而噪声将增强。

通过支持多种不同的速率，向无线客户端提供一定的灵活性，客户端在 AP 蜂窝内移动时，其速率可能随信号质量而变化，这被称为动态速率调整（Dynamic Data Rata Scaling）。当客户端逐渐远离 AP，导致信号质量降低到低于特定的阀值时，其速率将从 11 Mbps 降低到 5.5 Mbps、2 Mbps，条件是 AP 允许在其蜂窝内使用这些速率。

如果 AP 支持速率 1 Mbps、2 Mbps、5.5 Mbps 和 11 Mbps，在 AP 蜂窝内是否只能使用一种速率呢？对于 IEEE 802.11 而言，答案是否定的，各个客户端可以使用任何一种数据率，但在给定的时刻，只有一个工作站可以在信道内发送数据，然而，可以根据传输或接收客户端的需求，每帧都使用不同的速率。

1.3.4 IEEE 802.11g

IEEE 802.11g 标准是建立在 IEEE 802.11b 的基础之上的，但提供的速率高得多，使用的调制技术也复杂得多，它还向后与 IEEE 802.11b 兼容，让使用这两种标准的设备能够协同工作。

遵循 IEEE 802.11g 标准的设备使用 2.4 GHz 频段，这与 IEEE 802.11b 相同，另外，也使用 3 个相同的彼此不重叠的 22 MHz 信道（信道 1、信道 6 和信道 11）。

IEEE 802.11g 使用被称为正交频分多路复用（Orthogonal Frequency Division Multiplexing，OFDM）的调制技术，设备支持 6 Mbps、9 Mbps、12 Mbps、18 Mbps、24 Mbps、36 Mbps、48 Mbps 和 54Mbps 的速率，这相对于 IEEE 802.11b 有很大的提高。

然而，为向后与只能使用 IEEE 802.11b 的设备兼容，也可以使用 IEEE 802.11b 调制技术和速率 1 Mbps、2 Mbps、5.5 Mbps 和 11 Mbps。

我们需要知道的是，向后与 IEEE 802.11b 兼容存在一个缺点：在同一个 AP 蜂窝内，不能同时使用 IEEE 802.11g 和 IEEE 802.11b 调制技术，如果有遵循不同标准的客户端，将使用它们都支持的调制技术。这意味着即使只有一个 IEEE 802.11b 客户端关联到 IEEE 802.11g AP，而后者支持 IEEE 802.11b，整个 AP 蜂窝也必须切换到 IEEE 802.11b 模式，在这种情况下，虽然 IEEE 802.11g 蜂窝支持高达 54 Mbps 的速率，但它最高只能使用 11 Mbps 的速率。

IEEE 802.11g 标准也支持动态速率调整，客户端在 AP 附近时可使用 54 Mbps 的速率，但随着它们远离 AP，可调整到更低的速率。

IEEE 802.11g 采用的 OFDM 能够提供 52 个子载波信道（其中 48 个用于数据传输），所采用的 64QAM 编码方式能够在 8 bit 数据中有效传输 6 bit 数据，64QAM 编码每次传输提供 3/4 的码率（即有效数据容量）一次传输占用的时间固定为 4 μs，IEEE 802.11g 能提供的最大速率计算如下：

$$\frac{1}{4\ \mu s} \times 48 \times 6\ \text{bit} \times \frac{3}{4} = 54\ \text{Mbps}$$

1.3.5　IEEE 802.11a

IEEE 802.11a 标准规定 WLAN 使用 5 GHz 的未经许可的国家信息框架（U-NII）频段，实际上，FCC 将该频段分成了 3 个更小的频段，用于以下不同的用途。

- 低频段：5.15～5.25 GHz，供室内使用；
- 中频段：5.25～5.35 GHz，供室内和室外使用；
- 高频段：5.725～5.825 GHz，供室外使用。

在上述每个频段内，IEEE 802.11a 使用 4 个互不重叠的信道，每个信道的宽度为 20 MHz，这意味着在 WLAN 环境中可以使用 4、8 或 12 个互不重叠的信道。例如，如果要求更高的 AP 密度，可能需要有更多的信道可供使用。

IEEE 802.11a 标准支持动态速率调整，可使用 6 Mbps、9 Mbps、12 Mbps、18 Mbps、24 Mbps、36 Mbps、48 Mbps 和 54 Mbps 的速率。即使使用最高的速率 54 Mbps，通常，IP 最大吞吐量也只有约 30 Mbps，同 IEEE 80211b 和 IEEE 802.11g 一样，仅当离 AP 较近时才能获得较高的速率，当客户端逐渐远离 AP 时，必须使用越来越低的速率。

虽然 IEEE 802.11a 标准使用的速率和调制技术与 IEEE 802.11g 相同，但这两种标准是不兼容的。实际上，IEEE 802.11a 同 IEEE 802.11g 都不兼容，因为它使用的频段完全不同，在同一个区域内，遵循 IEEE 802.11a 和 IEEE 802.11b/g 的设备可以共存，条件是 AP 分别为采用每种标准的设备提供服务。

1.3.6　IEEE 802.11n

IEEE 802.11n 的提出是为增加 IEEE 802.11 设备的吞吐量，而不是简单地建立高比特率的无线传输能力。IEEE 802.11n 除了提供更高的比特率，还改变了 IEEE 802.11 设备之间通信的帧格式。本小节将介绍 IEEE 802.11n 的关键特性，包括 MIMO、无线增强特性和 MAC 增强特性。IEEE 802.11g 和 IEEE 802.11b 运行在 2.4 GHz 的频段或者 IEEE 802.11a 运行在 5 GHz 的频段上。而 IEEE 802.11n 工作在 2.4 GHz 或 5 GHz，或者同时两个频段上，从而提供了对 IEEE 802.11a/b/g 的向下兼容性。目前市场上绝大多数的 WiFi 设备和无线接入点都支持双频段（2.4 GHz 和 5 GHz）。利用 5 GHz 的 IEEE 802.11n 将能够为商业级用户提供更大的接入容量和更不易受干扰的频段。

基于 IEEE 802.11n 的无线解决方案利用如下几项技术来提供网络高性能、高可靠性和高可预言性。

- 多输入多输出（Multiple Input Multiple Output，MIMO）技术；
- 数据包聚合（Packet aggregation）技术；
- 通道绑定（Channel binding）技术。

上述三项关键技术结合起来能够让 IEEE 802.11n 提供 5 倍于 IEEE 802.11a/b/g 的网络性能。在同时传 2 路流的情况下，IEEE 802.11n 的最高无线接入速率目前为 300 Mbps，实际吞吐量可以超过 150 Mbps；将来为 IEEE 802.11n 同时传 4 路流时，IEEE 802.11n 的最高无线接入速率目前为 600 Mbps，实际吞吐量可以超过 300 Mbps。

1．MIMO

多输入多输出（MIMO）技术是 IEEE 802.11n 的核心。在传统单输入单输出无线传输中，接收的无线信号中携带的信息量的多少取决于接收信号的强度超过噪声强度的多少，也就是信噪比（Signal-to-Noise Ratio，SNR）。SNR 用分贝（dB）来表示，信噪比越大，信号能承载的信息量就越多，在接收端复原的信息量也越多。

一旦达到了允许信息交换的最小 SNR，额外的 SNR 可以用来增加信息速率，增加距离，或者二者均增加一些。MIMO 技术利用其他技术来改进接收端的 SNR，其中一项技术叫作传输波束成形。当有多个发射天线时，可以调整从各个天线发出的信号，使得接收端信号强度有显著的改善，该技术一般用于接收端只有单天线和表面反射障碍较少（如空旷环境）的情况。

要了解传输波束成形，可以认为无线信号是一种具有特定波长的波形。当从不同的天线发送两个无线信号时，这些信号在接收端天线进行叠加，如图 1-24 所示。由于传播的路径不同，两个信号在接收端存在相差，这种差异影响接收端总体的信号强度，通过微调发射端无线信号的相位，可以最大化接收端信号强度，即增加 SNR，这就是传输波束成形的工作——在接收端对发送端进行聚焦，如图 1-25 所示。

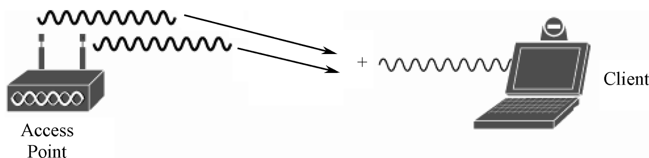


图 1-24　破坏性干扰

如果没有接收端接收信号的信息，传输波束成形很难在发射端完成。这种反馈只有 IEEE 802.11n 设备提供，IEEE 802.11a/b/g 设备均不能提供。为了最大化接收端的信号，接收端必须将反馈发往发射端，发射端才能够据此调整其发送的各个信号。该反馈不是立即的，而且只在很短的时间内有效。任何物理上的移动（发射端、接收端或周围的环境）都会使这些用户波束

成形的参数失效。2.4 GHz 的无线电的波长只有 120 mm，而 5 GHz 的无线电波只有 55 mm，因此，普通步行速度 1 m/s 会迅速地将接收端排除在波束成形的有效范围之外。

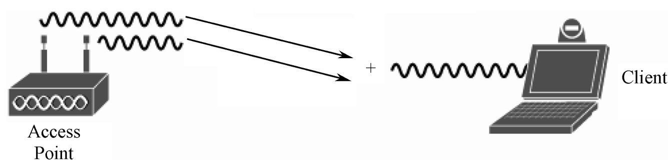


图 1-25　传输波束成形　（建设性干扰）

波束成形只适用于单接收者，在进行广播或者组播时无法对发射信号的相位进行优化。因此，在普通的网络应用中，波束成形的作用受到了限制，只能改善单播情况下接收端的 SNR。波束成形可以增加距离 AP 较远时的速率，但不能增加 AP 的覆盖范围，这在很大程度上是由从 AP 接收信标的能力决定的，而信标是一种组播传送，并不会从波束成形中受益。

对于典型的室内 WLAN 部署，如办公室，无线信号很少通过直接的最短的路径传送到接收端，因为发射端和接收端很少在视线范围之内，通常都会有隔板、门或者其他阻碍视线的障碍物，在信号穿透这些障碍物时，信号强度都会减弱。幸运的是，大多数障碍物都会像镜面反射光一样反射无线信号。

想象一下所有的金属表面，不论大小，实际上就是镜子。螺钉、门框和天花板吊顶等都是无线信号的反射体。可能在这些镜子中同时看到同一个 WLAN AP，有一些 AP 的图像是通过单个镜子直接反射的，而有一些可能是间接反射的，这种现象叫做多径效应，如图 1-26 所示。

当信号通过不同的路径传播到单个接收者时，信号到达时间取决于路径的长度，路径最短的信号最早到达，接下来是经过较长路径的信号的副本或者回声。当通过光速传播时，无线信号也是如此，第一个信号和其他副本到达的时延非常小，通常在纳秒级，但这个实验足以显著减弱单天线的信号，因为所有的副本都干扰第一个到达的信号。

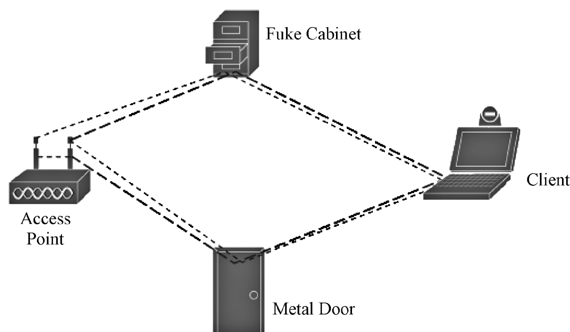


图 1-26　多径效应

MIMO 无线传输同时发送多个无线信号，并且利用多径效应。每个信号称为空间流。每个

空间流都从自己的天线发送，使用自己的发射器。由于在各个天线之间存在空间，每个信号都会通过略微不同的路径发送给接收端。这叫作空间分集。每个无线电波都可以传送不同于其他无线电波的数据流。接收端也有多个天线，每个天线有自己的无线电波接收器，每个接收器都对收到的信息进行独立解码，如图 1-27 所示。然后将各个无线电接收器收到的信号组合起来，通过复杂的运算，结果会比通过单个天线或者波束成形收到的信号好得多。MIMO 的优点之一就是显著改进 SNR，为 WLAN 系统设计者提供更高的灵活性。

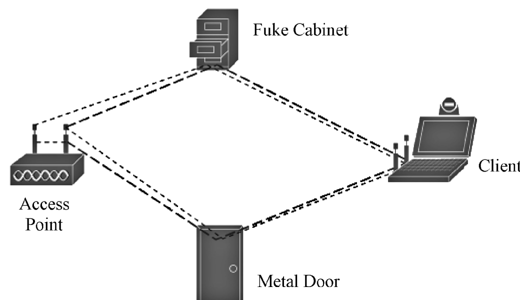


图 1-27　空间复用

MIMO 系统由系统中发射机及接收机数目命名。如 2×1 表示两个发射机及一个接收机。IEEE 802.11n 定义了一系列不同数目的发射机及接收机组合，从 2×1，即发送端波束形成，到 4×4。系统每增加一个发射机或接收机都会提高系统信噪比，然而，每个新增发射机或接收机增加的信噪比增益值会快速递减。从 2×1 到 2×2 到 3×2，信噪比的增加是非常明显的，然后，从 3×3 之后，信噪比增幅则比较小，多个发射机的应用体现了 MIMO 的第二个优势：即采用不同的空间信息流分别承载各自的信息，从而大大提高了数据传输速度。

2．物理射频增强

IEEE 802.11n 除了使用 MIMO 技术外，还使用增大信道，采用更高的调制速率，同时还减少冗余数据等射频技术，提高了 WLAN 的有效吞吐。下面将介绍新应用的射频技术及其对 WLAN 吞吐量的影响，首先介绍 20 MHz 和 40 MHz 信道。

原本的IEEE 802.11 直接序列射频和IEEE 802.11b 增强标准使用的信道带宽为22 MHz。IEEE 802.11a 及 IEEE 802.11g 使用 20 MHz 带宽信道。因为 IEEE 802.11g 是 IEEE 802.11b 的增强，故其也使用 22 MHz 带宽。吞吐量大小、带宽及射频信道是衡量射频效率的重要标准，称为频谱效率，以比特每赫兹（bit/Hz）为单位。IEEE 802.11b 的频谱效率为 0.5 bit/Hz，IEEE 802.11a 和 IEEE 802.11g 有稍高的频谱效率，在 54 Mbps 时可达到 2.7 bit/Hz。

使用完全相同的技术，IEEE 802.11a 和 IEEE 802.11g 的专有网络速率有时可到达 108 Mbps。这些专有系统使用简单的技术把 IEEE 802.11a/g 速率增强到原来的两倍，这种技术称为“信道绑定”，即同时利用两个信道传输。采用信道绑定，频谱效率跟原先的 IEEE 802.11a/g 相同，

而信道带宽是后者的两倍，这就提供了一种简单的将速率提高到两倍的方法。

IEEE 802.11n 使用 20 MHz 和 40 MHz 信道，与前面提到的专有产品类似，40 MHz 信道由两个相邻的 20 MHz 信道组成，若采用原先单独的 20 MHz 信道，信道在最低与最高频段保留一部分带宽避免信道间干扰，而当使用 40 MHz 绑定信道时，这些保留带宽可以用来传输信息。通过利用保留带宽，IEEE 802.11n 的信道应用效率更高，通常可比 20 MHz 带宽的两倍要稍高，如图 1-28 所示。

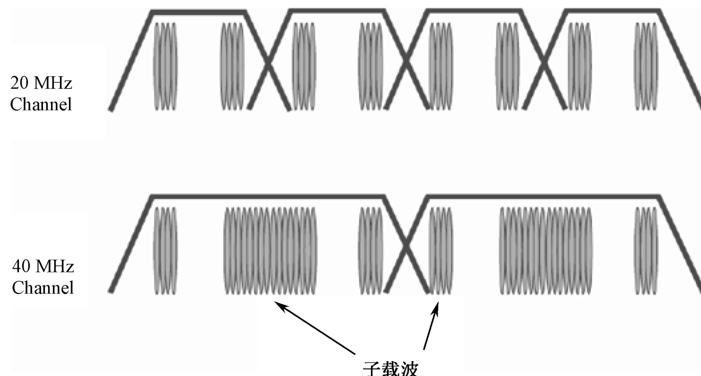


图 1-28　20 MHz 及 40 MHz 信道

最初的 IEEE 802.11 直接序列射频从发射端到接收端使用一个符号代表一个比特（或一组比特）。每个符号持续 1 微秒。每个符号由固定长度的 11 个码片组成。每个码片采用相移键控（PSK）调制。若采用 1 Mbps 的数据率，每微秒发送一个采用二进制相移键控技术调制的符号。同理，2 Mbps 每微秒发送两个采用四相移键控（QPSK）的符号。IEEE 802.11b 通过把更多比特信息编码成一个符号的同时，采用四相移键控，延伸了直接序列射频效率。因此，IEEE 802.11b 的速率达到 11 Mbps。

IEEE 802.11a/g 改变了信息在射频信号传输的方式，这些标准采用了一种新调制解调技术：正交频分复用（OFDM），OFDM 把信道分割成大量子信道，每个子信道采用各自子载波信号（如图 1-28 所示），每个载波信号可以独立携带信息，这样做的效果几乎等同于同时进行几个独立射频传输。

在 IEEE 802.11a/g 中，每个符号持续 4 微秒，包括 800 纳秒的保护间隔。若采用最高的传输速率 54 Mbps，每个符号要携带 216 比特信息，这些数字比特分布在 48 个子载波中。另外，当传输速率为 54 Mbps 时，每个符号包含 72 比特纠错信息，即一个符号达到 288 比特。为了把这么多比特包含在一个符号里，子载波采用 64 位四进制幅度调制（64QAM），为 IEEE 802.11b 的 16 倍调制速率。也就是说，每个子载波能携带 6 比特信息（包括数据信息及纠错码）。

与 IEEE 802.11a/g 一样，IEEE 802.11n 继续采用 OFDM 的 4 微秒信号。然而，IEEE 802.11n 把每个 20 MHz 信道的子载波数由 48 提高到 52。由此，对单一传输射频，速率可以达到最大 65 Mbps。IEEE 802.11n 为发射机提供了 8 个数据传输速率选项，同时发射机数目最多可达 4 个。

对于两个发射机，最大速率为 130 Mbps。3 个发射机可提供的最大速率为 195 Mbps。4 个则为 260 Mbps。在 20 MHz 信道中，IEEE 802.11n 一共能提供多达 32 个数据传输速率。

当采用 40 MHz 信道时，IEEE 802.11n 把可用子载波数提高到 108，从而为 1～4 个发射机分别提供的最大速率为 135 Mbps、270 Mbps、405 Mbps、540 Mbps，其中每个发射机有 8 个数据传输速率选项，对 4 个发射机而言，总共 32 个。

以上讨论的速率对所有子载波都基于相同的调制方式，如所有子载波采用 QPSK 或者 64 QAM，这与 IEEE 802.11a/g 技术是一致的。IEEE 802.11n 可以对不同的流采用不同调制方式。比如，一些数据流采用 QPSK，其他采用 16QAM，余下的则采用 64 QAM。通过这项技术，大大提高了可用速率的数目。然而，发射机需要接收机提供反馈信息才能判断对于不同的数据流应采用何种调制方法，而这在实际应用中是比较难实现的。

保护间隔是 OFDM 符号中用于减少符号间干扰的时间。在多径环境下，后一符号的前端比前一符号的末端更快到达接收机，从而导致符号间产生干扰。前、后符号从不同路径到达，前一符号尚未被接收机完全接收，后一符号却从一个更短路径到达，如图 1-29 所示。符号间干扰会降低射频链路的信噪比（SNR）。保护间隔是前、后符号间的一段空白时间，可以为迟到信号提供更长的缓冲时间。保护间隔长度根据多径状态选择。在最多 800 英尺的路径差异下，IEEE 802.11a/g 使用 800 纳秒的保护间隔。

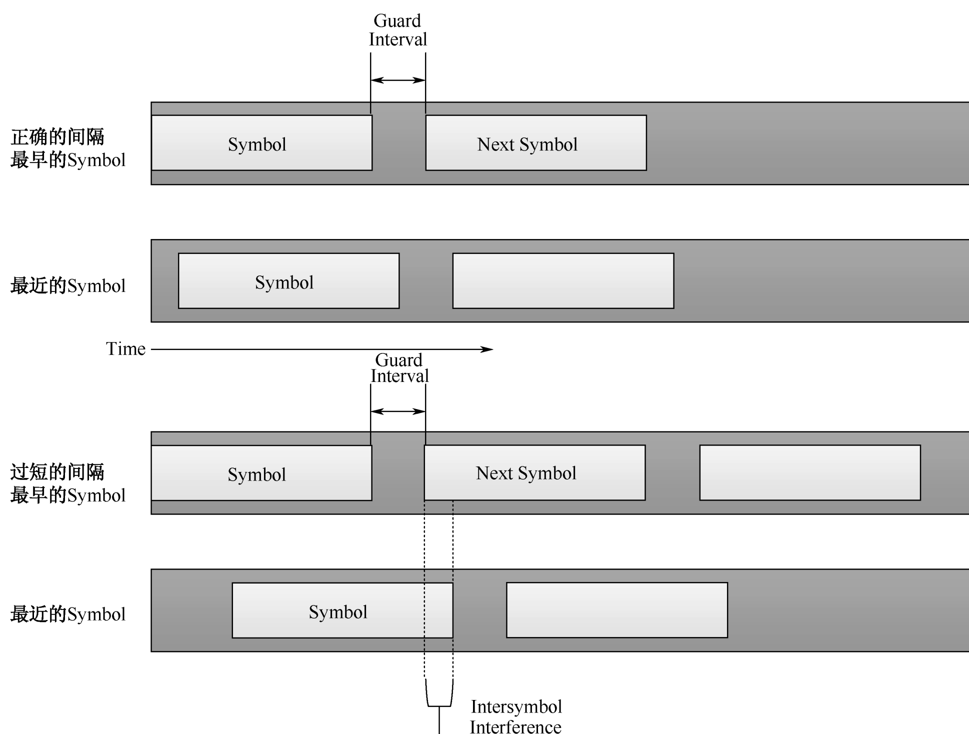


图 1-29 保护间隔

IEEE 802.11n 也默认采用 800 纳秒保护间隔。然而，假如在多径环境中，最长径与最短径差异远小于 800 英尺，IEEE 802.11n 采用 400 纳秒的保护间隔，这使符号长度从 4 微秒减少到 3.6 微秒。减少的符号时间会相应提高数据速率。对于 20 MHz 信道，采用 1～4 个发射机的最大数据速率分别为 72 Mbps、144 Mbps、216 Mbps 和 288 Mbps；对于 40 MHz 信道，则为 150 Mbps、300 Mbps、450 Mbps 和 600 Mbps。

3．速率计算方法

在 20 MHz 的带宽中，当采用长保护间隔、仅一个空间流时，56 个子载波中有效子载波为 52 个。采用 64QAM 的调制技术，8 bit 中的有效数据位为 6 bit，64QAM 的码率（Coding Rate）是 5/6，数据速率计算如下：

$$\frac{1}{4\ \mu s}\times 52\times 6\ \text{bit}\times\frac{5}{6}=65\ \text{Mbps}$$

如果其他条件相同，当采用短保护间隔时，速率计算方式如下：

$$\frac{1}{3.6\ \mu s}\times 52\times 6\ \text{bit}\times\frac{5}{6}=72.2\ \text{Mbps}$$

如果采用 40 MHz 的带宽，有效子载波为 108 个，当采用长保护间隔、仅一个空间流时，数据速率计算如下：

$$\frac{1}{4\ \mu s}\times 108\times 6\ \text{bit}\times\frac{5}{6}=135\ \text{Mbps}$$

当采用短保护间隔时：

$$\frac{1}{3.6\ \mu s}\times 108\times 6\ \text{bit}\times\frac{5}{6}=150\ \text{Mbps}$$

如果空间流的数量为多个，则乘以数量即可，最大数量为 4，因此 IEEE 802.11n 的最大数据传输速率为 150×4=600 Mbps。

1.3.7　IEEE 802.11ac

IEEE 802.11ac 作为 IEEE 的新标准，借鉴并优化了 IEEE 802.11n 的优点，它是更快且更易扩展的 IEEE 802.11n 版本，IEEE 802.11ac 结合了无线技术的灵活和千兆以太网的高容量。

IEEE 802.11ac 通过以下三个方面的进步来达到其基础速度。

- 更多的信道带宽绑定：从 IEEE 802.11n 的最大 40 MHz 增加到如今的 80 MHz 甚至 160 MHz。
- 密集调制模式：从 IEEE 802.11n 的 64 阶正交调幅（QAM）到如今的 256 阶正交调幅（达到 33%的增速，覆盖范围仍然不变）
- 更多的多输入多输出空间流：同 IEEE 802.11n 最多 4 个空间流相比，IEEE 802.11ac

能够达到 8 个空间流，实现 100%的增速。

IEEE 802.11ac 仅能工作在 5 GHz 频段，所以双频段的无线接入点和客户端会继续在 2.4 GHz 上使用 IEEE 802.11n，IEEE 802.11ac 客户端能够在不太拥挤的 5 GHz 频段工作。

思科第二代 IEEE 802.11ac 产品还会推出一种新的技术，多用户 MIMO（Multi User MIMO，MU-MIMO）。IEEE 802.11n 就像一个以太网的集线器，在同一时间只能向所有端口转发一个数据帧，MU-MIMIO 允许一个无线接入点在一个时间内使用相同的频带向多个用户发送多个帧，这类似于一台无线交换机。

下面以一个 80 MHz 频宽的信号为例，子载波数为 234 个，经过 256 阶正交调幅，数据码率为 1，以短保护间隔及常见的 3 个空间流发送，IEEE 802.11ac 的速率计算如下：

$$\frac{1}{3.6\ \mu s} \times 234 \times 8\ \text{bit} \times \frac{5}{6} \times 3 = 1\,300\ \text{Mbps}$$

当 IEEE 802.11ac 采用 160 MHz 频宽的信号时，子载波数达到 2×234=468 个，采用短保护间隔，以最大的 8 个空间流发送数据，能够达到传输的最大速率为：

$$\frac{1}{3.6\ \mu s} \times 2 \times 234 \times 8\ \text{bit} \times \frac{5}{6} \times 8 = 6\,933\ \text{Mbps}$$

1.3.8 其他 IEEE 802.11 标准

IEEE 还制定了其他属于 IEEE 802.11 系列的无线局域网标准，虽然本文不涉及这些标准，但我们应该知道存在下述标准。

- IEEE 802.11e：针对 WLAN 服务质量（QoS）；
- IEEE 802.11i：针对安全性改进。

注释：标准中使用的英文大小写有不同的含义，小写的英文字母代表非独立的标准，它无法脱离母标准而独立存在，大写字母则代表独立的规范。例如，IEEE 802.11a 是在 IEEE.11 中增加的新条款，无法独立存在，因此用小写字母 a 表示；而 IEEE 802.1Q 与 IEEE 802.1X 等标准，本身就是独立完整的规范说明书，因此用大写字母表示。

1.4 以太网供电

无线接入点和网络中的其他节点一样，必须有电才能运转，电的来源有两个：

- 外置交流电适配器；
- 通过网络数据电缆的以太网供电（Power over Ethemet，PoE，直流电）。

外置交流电适配器插在墙壁的交流电插座上，给 AP 提供 48 V 的直流电，这些适配器通常被称为“壁瘤”，在没有其他电源可用的情况下很方便。然而，如果适配器所在的房间或插座停电，无线接入点将无法运行。

Power over Ethernet 也叫内置电源（Inline Power），提供了一种更完美的解决方案，通过提供以太网链路的非屏蔽双绞线给无线接入点提供 48 V 的直流电。Catalyst 交换机本身就是直流电的提供者，除非需要使用交流电适配器作为冗余电源，否则不需要其他电源。

PoE 的好处在于，可对其进行管理和监控，并且只给无线接入点供电。事实上，这种功能不仅限于 Cisco 无线接入点或 IP 电话，能够以兼容方式请求和使用内置电源的设备都能够使用这种功能。如果将常规计算机连接到这种交换机端口，交换机将不会给它供电，因为它不能以兼容的方式请求和使用内置电源，Catalyst 交换机还可以连接不间断电源（UPS），这样，即使常规交流电出现故障，交换机也能持续获得并提供电力，这让无线、IP 电话等设备在停电期间仍可使用。

1.4.1　PoE 的工作原理

当 Catalyst 交换机被设计为能够通过其以太网端口供电时，它才能这样做。交换机必须有一个或多个电源，能够提供连接的设备带来的额外载荷。很多平台都支持 PoE，包括 Catalyst 2960 PWR、Catalyst 3750-PWR、Catalyst 3560-PWR、Catalyst 4500 和 Catalyst 6500。

为连接的设备提供 PoE 的方法有以下两种。

- Cisco 内置电源（CILP）：在标准 IEEE 802.3af 出现前开发的 Cisco 专用方法；
- IEEE 802.3af：一种基于标准的方法，为厂商提供了互操作性。

随着应用的拓展，出现了一些较高功率的设备，为此，IEEE 在 IEEE 802.3af 基础上提出了 IEEE 802.1at 标准，也称为 IEEE Power over Ethernet Plus (PoE+)，作为 IEEE 802.3af 的升级版，可以提供最高 30 W 的功率，Cisco 扩展了 IEEE 的 PoE+标准，最高提供 60 W 的供电功率，即 UPoE 标准（Cisco Universal Power Over Ethernet）。目前，在 Cisco 的 Catalyst 4500E 与 3850 的平台上提供。

1.4.2　检测需供电的设备

当交换机端口处于 Down 状态时，交换机将在该端口上停止供电，然后交换机必须不断检测端口是否连接了需要供电的设备，如果是，交换机必须开始供电，让该设备能够初始化并正常运行，至此才建立以太网链路。

由于有两种 PoE 方法，Catalyst 使用这两种方法来检测需要供电的设备，在 IEEE 802.3af 中，交换机首先在铜质双绞线连接的传输和接收针脚提供较低的电压，然后通过测量针脚之间的电阻来检测电流是否来自设备，如果测量到电阻为 25 Ω，表明连接了一台需要供电的设备。

交换机还能够提供多种预定的电压，以检测相应的电阻值。需要供电的设备使用这些值来指出它所属的 5 种 IEEE 802.3 af 功率类别之一，知道这一点后，交换机便能够分配设备所需的最大功率，表 1-4 列出了这些功率类别。

表 1-4 IEEEE 802.3 af 功率类别

功率类别	最大功率 / W	说明
0	15.4	默认类别
1	4.0	可选类别
2	7.0	可选类别
3	15.4	可选类别
4	—	预留以后使用

如果交换机或需要供电的设备不支持或不执行可选功率类别发现，将使用默认类别，截至目前，第 4 类未用，留给以后的设备要求的功率超过当前 Catalyst 交换机能力时使用。

Cisco 内置电源设备发现采用的方法与 IEEE 802.3 af 截然不同，交换机向以太网双绞线电缆的传输线对发出 340 kHz 的测试音频，而不是提供电压并测量电阻。传输音频而不是直流电是因为交换机在供电前必须检测到支持内置电源的设备，否则，如果连接的是其他类型的设备，将可能被损坏。

当无线接入点或 IP 电话等需要供电的设备没有通电时，让以太网链路的传输和接收线对形成环路。当这种设备连接到内置电源交换机端口时，交换机能够“听到”环回的测试音频，从而确定连接的是一台需要供电的设备，并对其供电。

1.4.3 向设备供电

交换机首先给设备提供默认功率，例如，在 Catalyst 3750-24-PWR 上，IP 电话获得的功率为 15.4 W（直流电电压为 48 V，电流为 0.32 A）。

供电的方式有以下两种：

- 在 Cisco CILP 中，通过线对 2 和 3（RJ-45 针脚 1、2 和 3、6）提供 48 V 的直流电；
- 在 IEEE 802.3af 中，可通过线对 2 和 3（RJ-45）针脚 1、2 和 3、6 以及线对 1 和 4（RJ-45）针脚 4、5 和 7、8 供电。

这样设备将能够通电并建立以太网链路，提供给设备的功率可从默认值变为更合适的值，这有助于避免交换机将电力浪费在使用的功率比端口默认功率低得多的设备上，如果使用的是 IEEE 802.3af，可通过检测设备的功率类别来更改功率。

如果使用的是 Cisco CILP，交换机可尝试与设备交换 Cisco 设备发现协议（CDP）消息。如果返回了 CDP 信息，交换机便能够知道设备的类型（如 IP 电话）及其实际功率需求，然后，交换机就可以将功率降低到设备所需要的值。要了解这个过程，请看下面的示例 1。在这里，功率从 15 000 mW 降低到了 6 300 mW，这些输出是使用命令 debug ilpower controller 和 debug cdp packets 得到的。

示例 1：显示功率调整过程。

```
30w1d: ILP Start PHY Cisco IP phone detection（ Fa0/6） Okay
30w1d: ILP Shut off ILP detection（ Fa0/6）
30w1d: ILP State_Machine（ Fa0/6）: State= ILP_SHUT_OFF_S, Event= GO_SHUT_OFF_EV
30w1d: ****Power controller address 0x42****
30w1d: Reg 0x0  = 0
30w1d: Reg 0x1  = F6
30w1d: Reg 0x2  = 0
30w1d: Reg 0x4  = 0
30w1d: Reg 0x10 = 0
30w1d: Reg 0x12 = AA
30w1d: Reg 0x13 = F
30w1d: Reg 0x14 = 77
30w1d: Reg 0x17 = 80
30w1d: ************************************

30w1d: ILP Start PHY Cisco IP phone detection（ Fa0/6） Okay
30w1d: ILP CLI 'no shut' handling（ Fa0/6） Okay
30w1d: ILP Start PHY Cisco IP phone detection（ Fa0/6） Okay
30w1d: ILP Start PHY Cisco IP phone detection（ Fa0/6） Okay
30w1d: ILP CLI 'no shut' handling（ Fa0/6） Okay
30w1d: CDP-PA: version 2 packet sent out on FastEthernet0/6
30w1d: ILP State_Machine（ Fa0/6）: State= ILP_SHUT_OFF_S, Event= CLI_START_DETECT_EV
30w1d: ****Power controller address 0x42****
30w1d: Reg 0x0  = 8
30w1d: Reg 0x1  = F6
30w1d: Reg 0x2  = 0
30w1d: Reg 0x4  = 7
30w1d: Reg 0x10 = 0
30w1d: Reg 0x12 = AA
30w1d: Reg 0x13 = F
30w1d: Reg 0x14 = 77
30w1d: Reg 0x17 = 80
30w1d: ************************************

30w1d: ILP Power Off at（ Fa0/6） Okay
30w1d: ILP After Power Off at（ Fa0/6）, port re-config  Okay
```

```
30w1d: ILP Start Power Controller phone detection（ Fa0/6） Okay
30w1d: ILP Start PHY Cisco IP phone detection（ Fa0/6） Okay
30w1d: ILP State_Machine（Fa0/6）: State= ILP_DETECTING_S, Event= CLI_START_ DETECT_EV
30w1d: ****Power controller address 0x42****
30w1d: Reg 0x0  = 8
30w1d: Reg 0x1  = F6
30w1d: Reg 0x2  = 0
30w1d: Reg 0x4  = 7
30w1d: Reg 0x10 = 0
30w1d: Reg 0x12 = AA
30w1d: Reg 0x13 = F
30w1d: Reg 0x14 = FF
30w1d: Reg 0x17 = 80
30w1d: ************************************

30w1d: CDP-PA: Packet received from NIC-Office-1231 on interface FastEthernet0/4
30w1d: **Entry  found in cache**
30w1d: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to down
30w1d: %SYS-5-CONFIG_I: Configured from console by vty0（202.120.80.1）
30w1d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down
30w1d: ILP State_Machine（Fa0/6）: State= ILP_DETECTING_S, Event= PHY_CSCO_ DETECTED_EV
30w1d: ****Power controller address 0x42****
30w1d: Reg 0x0  = 8
30w1d: Reg 0x1  = F6
30w1d: Reg 0x2  = 0
30w1d: Reg 0x4  = F
30w1d: Reg 0x10 = 0
30w1d: Reg 0x12 = AA
30w1d: Reg 0x13 = F
30w1d: Reg 0x14 = FF
30w1d: Reg 0x17 = 80
30w1d: ************************************

30w1d: %ILPOWER-7-DETECT: Interface Fa0/6: Power Device detected: Cisco PD
30w1d: ILP Power apply to（ Fa0/6） Okay
30w1d: ILP Start PHY Cisco IP phone detection（ Fa0/6） Okay
30w1d: ILP Power Accounting REQ_PWR（ Fa0/6） Okay sys_used=26820
```

```
30w1d: ILP State_Machine（ Fa0/6）: State= ILP_CSCO_PD_DETECTED_S, Event= IEEE_PWR_GOOD_EV
30w1d: ****Power controller address 0x42****
30w1d: Reg 0x0   = 0
30w1d: Reg 0x1   = F6
30w1d: Reg 0x2   = 0
30w1d: Reg 0x4   = 0
30w1d: Reg 0x10 = 88
30w1d: Reg 0x12 = AA
30w1d: Reg 0x13 = F
30w1d: Reg 0x14 = FF
30w1d: Reg 0x17 = 80
30w1d: ************************************

30w1d: ILP State_Machine（ Fa0/6）: State= ILP_PWR_GOOD_USE_IEEE_DISC_S, Event= PHY_LINK_UP_EV
30w1d: ****Power controller address 0x42****
30w1d: Reg 0x0   = 8
30w1d: Reg 0x1   = F6
30w1d: Reg 0x2   = 0
30w1d: Reg 0x4   = 7
30w1d: Reg 0x10 = 88
30w1d: Reg 0x12 = AA
30w1d: Reg 0x13 = F
30w1d: Reg 0x14 = FF
30w1d: Reg 0x17 = 80
30w1d: ************************************

30w1d: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to up
30w1d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
30w1d: CDP-PA: Packet received from Lib-4500 on interface GigabitEthernet0/1
30w1d: **Entry    found in cache**
30w1d: CDP-PA: version 2 packet sent out on FastEthernet0/2
30w1d: CDP-PA: version 2 packet sent out on FastEthernet0/4
30w1d: CDP-PA: version 2 packet sent out on GigabitEthernet0/1
30w1d: CDP-PA: Packet received from NIC-Office-1231 on interface FastEthernet0/4
30w1d: **Entry    found in cache**
30w1d: CDP-PA: version 2 packet sent out on FastEthernet0/6
```

1.4.4 配置 PoE

PoE 的配置很简单，每个交换机在供电前自动检测连接的设备是否支持内置电源，也可以禁用该特性，确保端口不会检测和提供内置电源。默认情况下，每个端口都尝试发现支持内置电源的设备，要改变这种行为，可以使用下面的接口配置命令：

```
Switch（config）# interface    mod/num
Switch（config-if）# power inline {auto [max mini-watts] |static [max mini-watts] |never}
```

默认情况下，每个交换机接口都配置为 auto 模式，自动检测设备和功率，另外，默认功率为 15.4 W，可以将最大功率修改为 max mini-watts（取值为 4 000～15 400）。

如果连接的设备不能与任何一种设备发现方法交互，可在配置交换机端口时使用关键字 static。同样，可用 max mini-watts 来设置提供的最大功率，如果没有指定，将使用默认功率 15.4 W。

如果要在端口上禁用 PoE，可使用关键字 never，这样，将不会在该端口上检测需要供电的设备，也不会供电。

1.4.5 查看 PoE

要查看交换机端口的 PoE 状态，可使用下面的 EXEC 命令：

```
Switch# show power inline [mod/num]
```

示例 2 是该命令的一些输出结果。如果功率类别为 n/a，表明使用的供电方法为 Cisco CILP 或者没有供电设备连接；否则，将显示 IEEE 802.3af 功率类别（0～4）。

【警告】

Catalyst 交换机在端口上通电后等待 4 s，看是否有设备激活，如果没有，将在该端口上断电。

示例 2：

```
NIC-Hall1#sh power inline
Available:370.0（w）    Used:65.0（w）    Remaining:305.0（w）

Interface Admin    Oper          Power     Device                    Class Max
                                 （Watts）
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1         auto     off              0.0          n/a                     n/a          15.4
Fa0/2         auto     on               7.0          Ieee PD                 2            15.4
Fa0/3         auto     off              0.0          n/a                     n/a          15.4
```

```
Fa0/4    auto   off    0.0    n/a                 n/a   15.4
Fa0/5    auto   off    0.0    n/a                 n/a   15.4
Fa0/6    auto   off    0.0    n/a                 n/a   15.4
Fa0/7    auto   off    0.0    n/a                 n/a   15.4
Fa0/8    auto   off    0.0    n/a                 n/a   15.4
Fa0/9    auto   off    0.0    n/a                 n/a   15.4
Fa0/10   auto   on     7.0    Ieee PD             2     15.4
Fa0/11   auto   off    0.0    n/a                 n/a   15.4
Fa0/12   auto   off    0.0    n/a                 n/a   15.4
Fa0/13   auto   on     7.0    Ieee PD             2     15.4
Fa0/14   auto   off    0.0    n/a                 n/a   15.4
Fa0/15   auto   on     7.0    Ieee PD             2     15.4
Fa0/16   auto   on     15.0   AIR-LAP1242AG-C-K9  3     15.4
Fa0/17   auto   off    0.0    n/a                 n/a   15.4
Fa0/18   auto   off    0.0    n/a                 n/a   15.4
Fa0/19   auto   on     15.0   AIR-LAP1242AG-C-K9  3     15.4
Fa0/20   auto   off    0.0    n/a                 n/a   15.4
Fa0/21   auto   off    0.0    n/a                 n/a   15.4
Fa0/22   auto   off    0.0    n/a                 n/a   15.4
Fa0/23   auto   on     7.0    Ieee PD             2     15.4
Fa0/24   auto   off    0.0    n/a                 n/a   15.4
```

【警告】

如果交换机端口原来连接的是无线接入点或 IP 电话，在将其拆下并插入常规以太网设备时一定要小心。在设备拆下后的 4 s 内，仍将会供电，如果在此期间插入不支持内置电源的设备，将可能被损坏，在拆下设备后，等待 10 s 再将其他设备连接到同一个端口。

第2章



无线网络架构及设计

本章要点

- WLAN 安全
- AP 的关联和漫游
- 蜂窝布局和信道的使用
- 用户设备选型

2.1　WLAN 安全

作为基本服务集（BSS）的中央枢纽，AP 实际上为其覆盖范围内的客户端管理 WLAN，无线客户端发送的数据流都必须经过 AP，才能到达当前 BSS 内的其他 WLAN 客户端或位于其他地方的有线客户端，如图 2-1 所示，客户端之间不能直接通信。

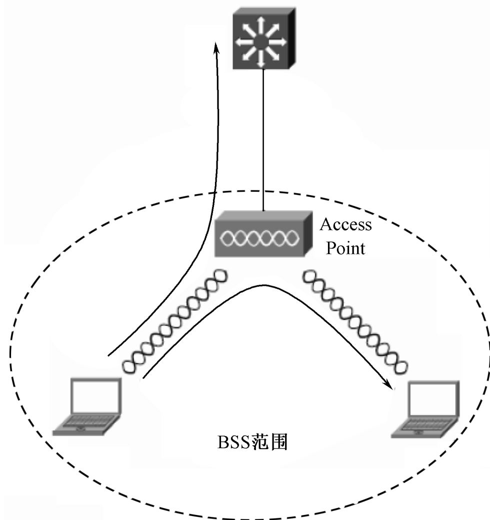


图 2-1　AP 充当 WLAN 中的中心连接点

显然，各种形式的安全非常适合在 AP 处实现，例如，AP 可以通过对客户进行认证来控制 WLAN 成员资格，如果客户不能通过认证，将不允许使用无线网络。另外，AP 及其客户端可协同工作，以确保在它们之间传输的数据安全，否则，在空中传输的数据可能被截取和利用。

客户端在建立其无线连接时，必须找到可到达并提供成员资格的 AP，客户端必须按如下顺序协商成员资格和安全措施，如图 2-2 所示。

① 使用与 AP 匹配的 SSID；

② 向 AP 认证；

③ 使用一种分组加密方法确保数据的隐秘性，这步是可选的；

④ 使用一种分组认证方法确保数据的完整性，这步也是可选的；

⑤ 建立同 AP 的关联。

第 1 章讨论过，SSID 字符串用于将客户端同合适的 WLAN（以及有线网络中的 VLAN）匹配。如果客户端的 SSID 与某个 AP 使用的 SSID 相同，它便可以开始同该 AP 通信。SSID 并不是一种安全措施，而只是用于将 WLAN 划分成逻辑用户组。

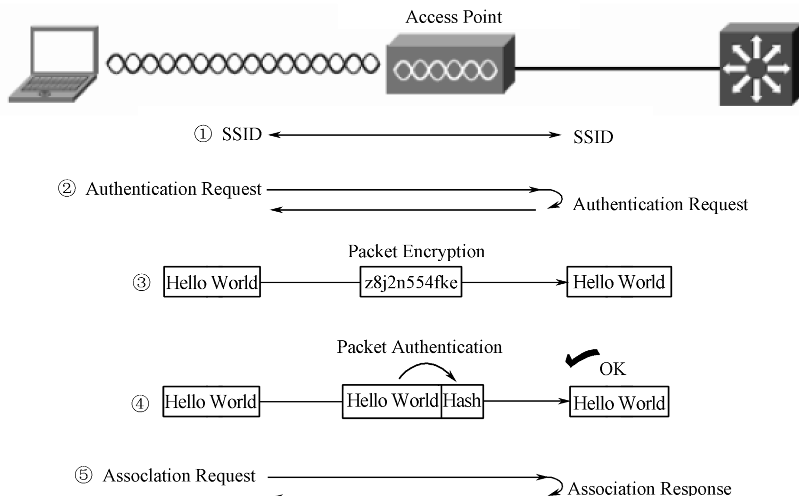


图 2-2　确保无线局域网连接安全的基本过程

IEEE 802.11 客户端和 AP 必须确定的两点是认证和加密。很多方法可用于进行认证、加密或两者，接下来的几小节将介绍这些方法。

2.1.1　以前的安全性

在 IEEE 802.11 网络中，客户端必须使用下述方法之一向 AP 认证。

- 开放认证：不使用任何认证方法，任何客户端都可以随便访问 AP；
- 共享密钥（PSK）：在客户端和 AP 上静态地指定相同的秘密密钥，如果密钥相同，客户端将被允许访问 AP。

在这两种认证方法中，认证过程都将在 AP 处结束，换句话说，AP 本身有足够的信息来独立地确定客户端是否有访问权。开放认证和 PSK 被视为以前的认证方法，因为它们的可扩展性差，且不一定安全。

开放认证是默认设置，无法对客户端进行筛选，任何客户端都可以加入网络，而无须提供任何凭证，实际上，SSID 是需要提供的唯一凭证。虽然这使得认证工作更容易，但几乎无法控制对 WLAN 的访问。另外，开放认证没有提供对通过 WLAN 传输的数据进行加密的措施。

预共享密钥认证使用一个存储在客户端和 AP 中的无线等效协议（Wireless Equivalence Protocol，WEP）密钥，当客户端要加入 WLAN 时，AP 向它发送一个挑战短语，客户端必须使用挑战短语和 WEP 密钥计算出一个可公开共享的值，并将其发回给 AP，AP 使用自己的 WEP 密钥计算一个类似的值，如果这两个值相同，客户端便通过了认证。

在使用预共享密钥（常被称为静态 WEP 密钥）认证时，WEP 密钥也被用作加密密钥，WLAN 在发送每个分组时，将把分组的内容和 WEP 密钥提供给加密进程，远端收到分组后，

将使用相同的 WEP 密钥对其进行解密。

预共享密钥认证比开放认证安全，但存在以下两个缺点：

- 可扩展性不佳，因为必须在每台设备上配置一个很长的密钥字符串；
- 不是很安全。

静态密钥的使用时间非常长，直到手工重新配置了新密钥为止，密钥的使用时间越长，恶意用户便有更长的时间来收集从它派生而来的数据，并最终通过逆向过程破解密钥。众所周知，静态 WEP 密钥是可以破解的，因此不推荐使用这种认证方法。

2.1.2　基于 EAP 的安全方法

无线安全已发展到使用其他更健壮方法的阶段，AP 可使用各种利用外部认证和授权服务器及其用户数据库的认证方法。

可扩展的认证协议（Extensible Authentication Protocol，EAP）是众多无线安全方法的基础，这些方法的缩略语的末尾都是一致的，如 EAP、PEAP 和 LEAP。EAP 是在 RFC 3748 中定义的，最初用于处理 PPP 用户认证，鉴于其可扩展性，它非常适合用于各种安全环境，RFC 4017 定义了用于 WLAN 中的 EAP 变种。

EAP 最初用于 PPP 通信，而不是无线认证，IEEE 802.1X 协议可用于基于端口的认证，即对认证用户是否能够使用特定的交换机端口，通过 IEEE 802.1X，甚至可以在用户获得网络连接性之前，在第二层对其进行认证，WLAN 可使用 IEEE 802.1X 在第二层实现 EAP。

在无线局域网中，可使用 LEAP、PEAP、EAP-TLS 和 EAP-FAST 这些安全方法，由于存在众多的安全方法，使得难以记住它们的功能和强项，只需记住这样一点，即它们都是基于 EAP 的，但使用不同的凭证来认证无线用户。

有些基于 EAP 的方法添加了其他安全功能，从而超越了认证的范畴，在接下来的几小节中，将讨论各种方法，读者将逐渐明白这一点。

1．LEAP

Cisco 开发了一种名为轻量级 EAP（LEAP 或 EAP-Cisco）的协议，以克服 IEEE 802.11 安全中的一些缺点。在使用 LEAP 时，AP 使用一个外部的远程验证拨号用户服务（RADIUS）的服务器来实际处理客户端认证，实际上，AP 和无线客户端将借助 RADIUS 服务器，通过交换挑战和响应来相互认证，使用的凭证是用户名和密码。

LEAP 还辅以 WEP 密钥分配解决了无线数据的隐秘性问题，RADIUS 服务器动态地为每个无线客户端生成不同的 WEP 密钥，这在客户端每次认证时都要向其提供新的加密密钥，从而无须手工配置静态的 WEP 密钥。

2．EAP-TLS

EAP-TLS 方法是在 RFC 2716 中定义的，它使用传输层安全（Transport Layer Security，TLS）协议来确保客户端认证的安全，TLS 基于安全套接字层（SSL），后者常用于确保 Web 服务器会话的安全。EAP-TLS 使用数字证书作为认证凭证，这意味着每个 AP 和无线客户端都必须有一个证书，这些证书由一家认证机构（CA）颁发并签名。

EAP-TLS 还解决了无线数据隐秘性问题，这是通过在认证服务器要求客户端重新认证时自动生成 WEP 密钥实现的，每当无线客户端进行认证时，都将使用不同的 TLS 会话密钥，该密钥将被用于派生出唯一的 WEP 密钥，然后使用后者对无线数据进行加密。

3．PEAP

受保护的 EAP（PEAP 或 EAP-PEAP）类似于 EAP-TLS，它也是用 TLS 会话来确保认证安全的。PEAP 仅要求认证服务器有数字证书，以便服务器能够向客户认证，而对无线客户端的认证是使用 Microsoft 挑战握手认证协议第 2 版（MS-CHAPv2）进行的。

和 EAP-TLS 一样，使用 TLS 会话密钥派生出用于加密无线数据的 WEP 密钥，每当认证服务器要求客户端重新认证时，都将修改密钥。

4．EAP-FAST

通过安全隧道的 EAP 灵活认证（EAP Flexible Authentication via Secure Tunneling），EAP-FAST 是 Cisco 开发的一种无线安全方法，其名称中的 FAST 指的并非速度，而是在降低管理复杂度方面的灵活性，客户端不需要使用数字证书，也无须遵循严格的强密码策略。

EAP-FAST 在客户端和认证服务器之间建立一个安全隧道，在建立隧道时唯一使用的客户端凭证是受保护的接入凭证（Protected Access Credential, PAC），PAC 可由 PAC 服务器分配，也可在 EAP-FAST 协商期间自动创建，在隧道建立后，便可以使用户名和密码对客户端进行认证。

EAP-FAST 能够动态地派生出 WEP 密钥，以便对无线数据进行加密。

2.1.3 WPA

IEEE 802.11i 标准致力于无线安全的各个方面，甚至超越了客户端认证和使用 WEP 密钥确保数据隐秘性的范畴，在制定 IEEE 802.11i 标准期间，无线局域网厂商已走在前头，在尽可能多地实现该标准指定的功能，因此，WiFi 联盟根据 IEEE 802.11 草案的一些内容开发了 WiFi 受保护的接入（WiFi Protected Access，WPA）。

WPA 提供了下述无线局域网安全措施：

- 使用 IEEE 802. 1X 或预共享密钥进行客户端认证；
- 客户端和服务器之间的双向认证；
- 使用临时密钥完整性协议（Temporal Key Integrity Protocol, TKIP）确保数据隐秘性；
- 使用消息完整性校验（Message Integrity Check, MIC）确保数据完整性。

TKIP 利用无线客户端和 AP 嵌入现有 WEP 加密硬件，WEP 加密过程与以前相同，但 WEP 密钥的生成频率更高，而不是像在使用基 EAP 的认证方法时那样，在每次重新认证时生成 WEP 密钥。

实际上，TKIP 为每个分组生成新的 WEP 密钥，当客户适用于基于 EAP 的方法对客户端进行认证（或重新认证）时，将生成一个初始密钥，该密钥是通过混合发送方（客户端或 AP）的 MAC 地址和一个序列号生成的。在发送每个分组时，都将更新该 WEP 密钥。当客户端被要求重新认证时，将生成一个全新的 WEP 密钥，然后在发送每个分组时更新该密钥。

如果没有使用或不需要外部认证服务器，WPA 可使用预共享密钥进行认证，在这种情况下，客户端和 AP 在相互进行认证时将只使用该预共享密钥。数据隐秘性（加密）根本不使用该预共享密钥，而由 TKIP 负责进行快速加密密钥更新，以用于进行 WEP 加密。

对于通过无线网络发送的每个分组，将使用 MIC 进程来为其生成一个“指纹”，如果指纹是在分组发送前生成的，则收到分组后，该指纹将同分组的内容匹配。为何要给分组加上指纹呢?分组在空中传输时，可能被拦截、修改并重新发送，这是绝对不能允许发生的，通过添加指纹，可确保数据在网络中传输时的完整性。

对于每个分组，MIC 将生成一个散列码（密钥）——通过单向复杂算法得到的结果，MIC 密钥是使用加密前的分组内容以及源和目标 MAC 地址计算得到的，因此在传输路径中无法对其进行篡改。如图 2-2 所示，在原始分组中加入了 MIC 散列码，这样接收方将能够通过查看该散列码来确定分组是否被篡改过。

2.1.4　WPA2

WiFi 受保护的接入第 2 版（WPA2）是基于最终的 IEEE 802.11i 标准的，在安全措施方面，它在 WPA 的基础上做了多方面的改进。

在进行数据加密时，它使用的是最高级加密标准（Advanced Encryption Standard，AES）。AES 是一种健壮、可扩展的加密方法，美国国家标准和技术协会（NIST，www.nist.gov）已批准在美国政府机构中使用它，WPA2 也支持使用 TKIP 对数据进行加密，以便向后同 WPA 兼容。

在使用 WPA 和其他基于 EAP 的认证方法时，无线客户端必须向要访问的每个 AP 进行认证。如果客户端从一个 AP 移到另一个 AP，将需要不断进行认证，这很麻烦，WPA2 使用主动密钥缓存（Proactive Key Caching，PKC）解决了这个问题，客户端只需认证一次——向它遇到的第一个 AP 认证，只要客户端访问的其他 AP 都支持 WPA2，且被配置为属于一个逻辑组，就将自动传递缓存的认证信息和密钥。

2.1.5 无线认证方式总结

无线局域网安全方法比较如表 2-1 所示。

表 2-1 无线局域网安全方法比较

方　　法	使用的凭证	数据安全性
开放认证	无	无
静态 WEP	静态 WEP 密钥	WEP 加密（静态密钥）
LEAP	用户名 / 密码	WEP 加密（静态密钥）
EAP-TLS	数字证书	WEP 加密（静态密钥）
PEAP	服务器：数字证书 客户端:任何 EAP 方法	WEP 加密（静态密钥）
EAP-FAST	使用 PAC 来建立隧道 用户名 / 密码	WEP 加密（静态密钥）
WPA	任何基于 EAP 的方法或预共享密钥	WEP 加密（TKIP 为每个分组生成密钥） MIC 执行分组认证以确保完整性
WPA2	任何基于 EAP 的方法 预共享密钥 主动密钥缓存（在 AP 之间漫游时只需认证一次）	AES 加密或 TKIP MIC 执行分组认证以确保完整性

2.2 AP 的关联和漫游

无线客户端在同 AP 关联后，所有前往和来自客户端的数据都必须经过该 AP。第 1 章介绍过，客户端通过向 AP 发送关联请求消息来建立关联，如果客户端与 WLAN 兼容，即有正确的 SSID、支持相同的速率并通过了认证，AP 将使用关联应答进行响应。

只要客户端在当前 AP 的覆盖范围内，其同该 AP 的关联就将得到维持。请看图 2-3 所示的 AP 蜂窝，只要客户端在点 A 和 B 之间，就能够以可接受的质量接收 AP 的信号：在客户端走出该蜂窝（到达图中的 C 点）后，信号强度将低于可接受的阈值，导致客户端失去关联。

可以通过添加 AP 让客户端能够在更大的区域内移动。然而，必须仔细地部署 AP，让客户端能够在 AP 之间漫游。漫游指的是从一个 AP 将关联切换到与另一个 AP 关联，让无线连接在客户端移动时能够保持的过程。

在图 2-4 中，两个 AP 被并排地放置，它们使用相同的信道。使用单个信道来建立大型覆盖区域看起来很直观，但实际上，这是种糟糕的想法，因为客户端无法确定它在什么时候已离开一个 AP 的蜂窝，进入到另一个 AP 的蜂窝内。

AP 的信号在其蜂窝边缘并没有消失，它将继续传播直到最终消失，图 2-4 中的信号强度图就说明了这点，在 A 点，客户端能够同 AP1 建立关联，即使是在这里也能够收到来自 AP2 的信号，由于 AP2 和 AP1 使用的信道相同，因此这两个 AP 将相互干扰。

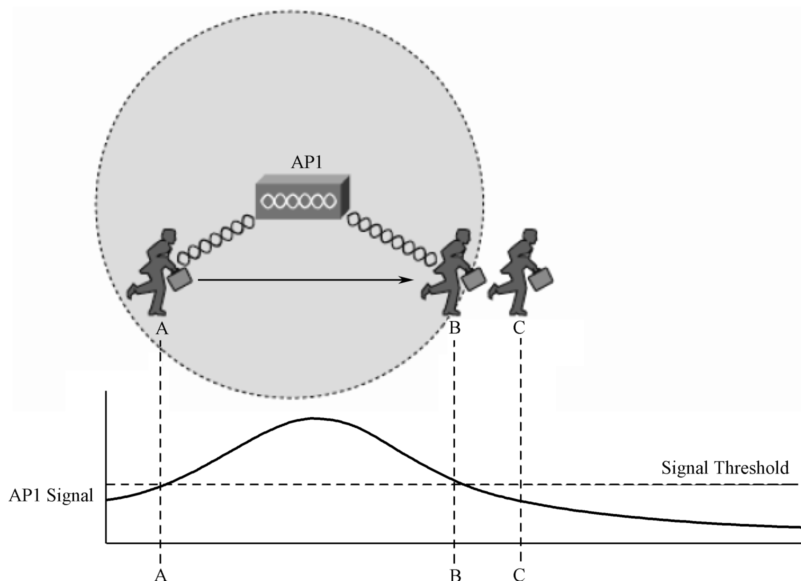


图 2-3　移动客户端在 AP 蜂窝内移动

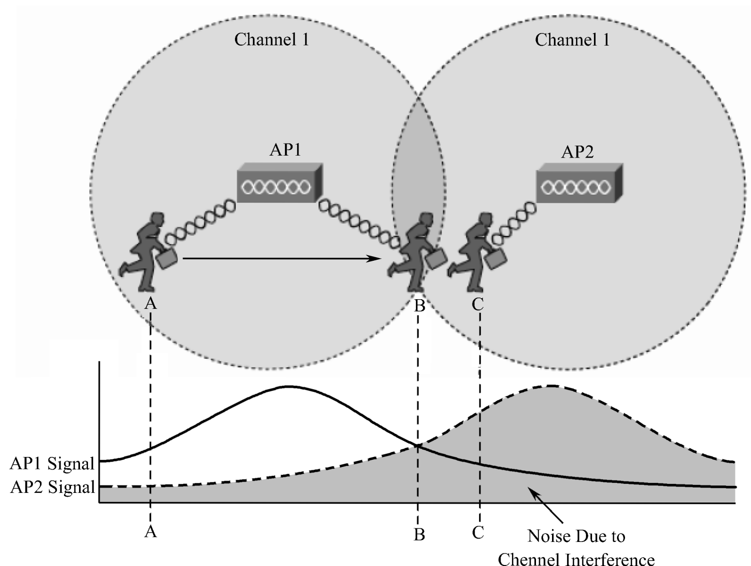


图 2-4　相邻 AP 使用相同信道

理想情况下，在图 2-4 中，当客户端移到 B 点时，应预测到需要漫游，即将关联从 AP1 切换到 AP2。在两个 AP 的信道相互干扰的情况下，可能无法进行明确的漫游，实际上，客户端可能无法在两个蜂窝内不受干扰地运行。

2.2.1 漫游过程

要让客户端能够漫游，必须满足的条件是什么？首先，必须将相邻 AP 配置为使用互不重叠的不同信道。例如，遵循 IEEE 802.11b 或 IEEE 802.11g 的 AP 只能使用信道 1、信道 6 和信道 11，同时使用信道 1 的 AP 不能与其他使用信道 1 的 AP 相邻，这就确保客户端在接收附近 AP 的信号时不受来自其他 AP 的信号干扰。

漫游过程完全是由无线客户端设备驱动而不是由 AP 驱动的，客户端可采取以下两种方法来确定何时进行漫游。

- 客户端可以在其需要漫游前主动搜索其他相邻 AP；
- 客户端可以在需要漫游时才搜索相邻 AP。

无线客户端根据各种条件确定漫游的时机，IEEE 802.11 标准没有解决这个问题，因此使用的漫游算法随厂商而异。另外，漫游算法通常使用的是“秘密配方”，因此，无法知道精确的阈值和条件。

在漫游算法中，使用的一些条件包括信号强度、信号质量、遗漏的信标数、由于冲突或干扰导致的错误等。选择这些条件通常是合乎逻辑的，因为它们说明了连接的整体质量。

由于不同的客户端使用不同的阈值，因此在蜂窝内的同一个位置，有些客户端可能尝试进行漫游，而有些不这样做。有些客户端选择在几乎收不到当前 AP 的信号时才进行漫游，而有些客户端在有更佳的 AP 时就进行漫游。换句话说，我们不要过多地考虑控制漫游算法的因素，而只需熟悉漫游过程即可。

客户端确定应该漫游后，它首先必须搜索潜在的新 AP，这是通过扫描其他信道以找到其他活动 AP 实现的，客户端采取以下两种方法来执行扫描过程。

- 被动扫描：客户端花时间来扫描其他信道，但只侦听来自可用 AP 的 IEEE 802.11 信标；
- 主动扫描：客户端花时间来扫描其他信道，同时发送 IEEE 802.11 探针请求帧来查询可用 AP。

当客户端采用被动扫描时，只需等待接收信标即可，因此非常适合用于低功率的嵌入式无线客户端。主动扫描让客户端具有控制权，因为必须发送探针并等待接收探针应答，通常，主动扫描比被动扫描可实现更高效的漫游，因为可以根据需要查询和识别 AP。

在图 2-5 中，对两个 AP 进行了正确的配置，使其使用互不重叠的信道 1 和信道 6，同时列出了两个 AP 的信号强度同客户端位置的关系图。在位置 A，客户端可以从 AP1 那里收到清晰的信号，因此它保持同该 AP 的关联。

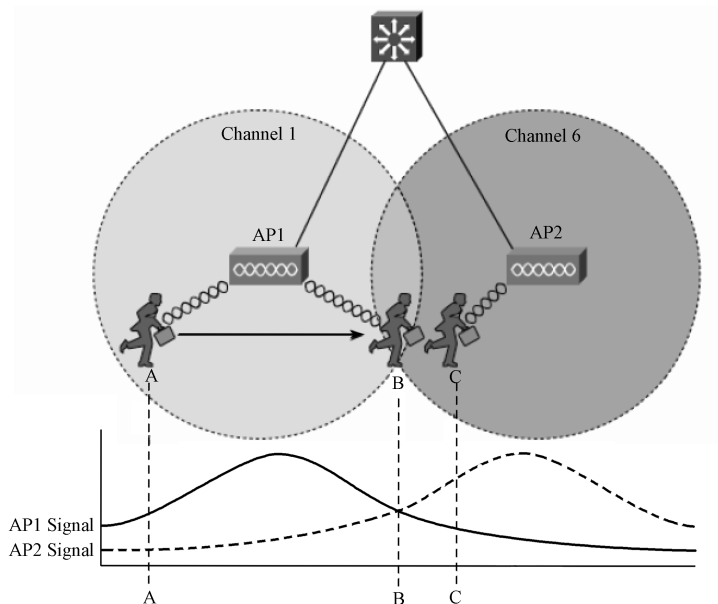


图 2-5　客户端在两个 AP 之间漫游

当客户端向位置 B 移动时，它发现 AP1 的信号不再是最优的，在此过程的某个位置，客户端开始查找更佳的 AP 以便同其关联，无线客户端采取以下两个步骤来完成这个过程。

- 第 1 步：客户端发送 IEEE 802.11 探针请求管理帧；
- 第 2 步：侦听的 AP 使用 IEEE 802.11 探针响应帧来应答客户，以通告自己的存在。

客户端并不知道将遇到的下一个 AP 使用的信道，因此它必须通过每个可能的信道发送探针，所以它必须花时间来调整发射器，使其远离当前 AP 的信道，以便能够扫描其他信道并发送探针。

我们可认为这类似于看电视，对当前节目感到厌烦或它接近尾声时，观众开始搜索其他信道以找到更好的节目。有一点需要记住：观众扫描信道时不能继续观看原来的节目，因此会错失该节目的部分内容。无线客户端与此相同，发射器在扫描其他信道时，通过原来的信道到来的分组将丢失，因为无法接收它们。因此，必须在延续当前信道和漫游到其他 AP 之间进行折中。

回到图 2-5，当客户端移到位置 B 附近时，在各种信道中发送 IEEE 802.11 探针请求帧。AP2 在信道 6 中收到探针请求后，它通过在信道 6 中发送探针应答来进行响应，客户端收到探针应答后，对其进行评估，以确定同哪个 AP 关联是最合适的。

现在，客户端必须进行漫游，并切换关联。在图 2-5 中，客户端到达位置 B 后仍同 AP1 关联，虽然它可能能够从 AP2 接收到更佳的信号。

首先，必须删除现有的关联，因为每个客户端不能同时与多个 AP 关联，客户端通过信道 1（AP1 使用的信道）向 AP1 发送 IEEE 802.11 解除关联消息，然后客户端便可以通过信道 6 向 AP2 发送关联请求，接下来 AP2 使用关联响应做出应答。

2.2.2 漫游的含义

正如图 2-5 暗示的，相邻 AP 连接到一个交换型网络，属于同一个 VLAN，因此，AP 之间的 IEEE 802.11 漫游实际上发生在第二层，可以将其视为类似于：客户计算机从连接到一台接入层交换机切换到连接到另一台接入层交换机的情况，但由于位于同一个 VLAN 中，这意味着在漫游期间，客户端的 IP 地址保持不变，这就提供了方便，因为当客户端关联到另一个 AP 时，无须花时间来获得新的 IP 地址。

在漫游过程中，客户端必须先解除原来的关联才能协商新关联，因此在一段较短的时间内，客户端没有同任何 AP 相关联，这实际上就是客户端无法发送或接收数据的离线时间。然而，第二层漫游的目标是确保离线时间尽可能短，以免对延迟敏感的应用受到负面影响。

有时候，在 WLAN 的规模很大时，最好增加新的 IP 子网和 VLAN。应将大型园区网划分成多个交换模块，以免出现跨越整个园区网的 VLAN，对 WLAN 来说也如此，因为它实际上只是对交换型网络的扩展。

如果 WLAN 被划分成多个 VLAN 和子网，无线客户端在漫游时可能跨越第三层边界，在这些边界上漫游时，客户端的 IP 地址可能发生变化。在这种情况下，漫游不仅需要发送 IEEE 802.11 探针和关联请求，客户端还需要请求并获得新的 IP 地址，因此离线时间将更长。

普通 AP 本身不支持第三层漫游，需要利用可在 IEEE 802.11 网络中部署的其他工具。这个问题可使用第 3 章（思科统一无线网络）介绍的无线基础设施来解决。

2.3 蜂窝布局和信道的使用

2.2 节通过介绍客户端在两个 AP 蜂窝之间移动阐述了有关漫游的基础知识，在大多数情况下，为覆盖大楼内合适的区域，需要多个 AP，因此，需要根据无线环境考虑蜂窝布局并配置更多的 AP。

例如，为覆盖仓库或大楼的整层，必须在整个空间内以相同的间隔放置 AP，为确定 AP 的位置，现场勘查至关重要，这样可以将 AP 放在不同的地方并进行实际的测量，在设计 WLAN 时，两个基本目标如下：

- 确定 AP 蜂窝的大小；
- 选择每个 AP 使用的信道。

接下来的几小节将介绍这些目标。

2.3.1 确定 AP 蜂窝的大小

AP 蜂窝的大小决定了需要购买并部署的 AP 数量，然而，设计方案并不能仅根据成本来

选择。当客户端移动或汇集在同一个地方时，AP 蜂窝的大小将影响 AP 的性能。

WLAN 是一种共享介质，在单个 AP 蜂窝内，与 AP 相关联的所有客户端将共享并争用带宽，如果蜂窝太大，可能有大量的客户端聚集在这里，并使用该 AP，如果缩小蜂窝，同时使用网络的客户端数量也将减少。

有关 AP 蜂窝应覆盖多少个客户端没有固定的经验规则，和交换型网络一样，限制客户端数量的因素是客户端使用的应用类型以及在给定时刻通过介质传输的数据量。

作为一个非常粗略的指导原则，可考虑将无线蜂窝的最大峰值吞吐量除以同时上网的客户端数量，得到每位用户的最大速率，同时应考虑 IEEE 802.11 封装和带宽争用带来的开销，当使用 IEEE 802.11b 时，单个 AP 的吞吐量通常可高达 6.8 Mbps，而 IEEE 802.11g 和 IEEE 802.11a 可高达 32 Mbps。

这意味着在包含 25 个客户端的 IEEE 802.11b 蜂窝内，每个客户端的最大吞吐量为 272 kbps（6.8 Mbps/25），当 IEEE 802.11a 或 IEEE 802.11g 蜂窝内包含 25 个客户端时，每个客户端的最大在吐量为 1.28 Mbps（32 Mbps/25）。

另外，在大型蜂窝内，当客户端远离 AP 时，其速率将降低，例如，当 IEEE 802.11b 客户端在 AP 附近时，可以使用最高的速率为 11 Mbps，随着客户端渐渐远离 AP，速率将降低到 5.5 Mbps，2 Mbps 和 1 Mbps，你可能希望客户端在蜂窝内能够使用最高的速率，这可以通过缩小蜂窝来实现。

一般而言，AP 蜂窝的大小取决于 AP 的发射功率，功率越高，覆盖范围越大。因此，必须调整 AP 的发射功率，以免其信号传播到附近使用相同信道的 AP 蜂窝内。

有关 AP 蜂窝大小和无线局域网现场勘察的更详细信息，请阅读 Cisco Airespace Installation, Administration and Maintenance（CAIAM）或 Cisco Aironet Wireless Site Survey（CAWSS）课程。

在确定 AP 蜂窝的大小和位置后，客户端应该能够在覆盖范围内的任何位置关联和漫游，如果一个 AP 出现故障，它原来覆盖的区域将变成静区。

显然，可以通过替换出现故障的 AP 来修复这个“洞”，如果能在 AP 出现了故障的第一时间发现的话，也可以对相邻的 AP 进行配置以增大其输出功率，从而使其覆盖范围包含这个“洞窝”。

2.3.2　WLAN 信道布局

为最大限度地减少信道之间的重叠和干扰，应避免相邻 AP 使用相同的信道，在 IEEE 802.11b 和 IEEE 802.11g 中，只能使用信道 1、信道 6 和信道 11，可以有规则地排列蜂窝，交替使用不同的信道，如图 2-6 所示。

然而，请注意在这些信道交叉的中央区域发生的情况——有一个没有被 RF 覆盖的小洞，如果客户端漫游时经过这个洞，可能立刻失去无线信号。另外，如果缩短蜂窝之间的距离，以覆盖这个洞，两个使用信道 1 的蜂窝将重叠，进而相互干扰。

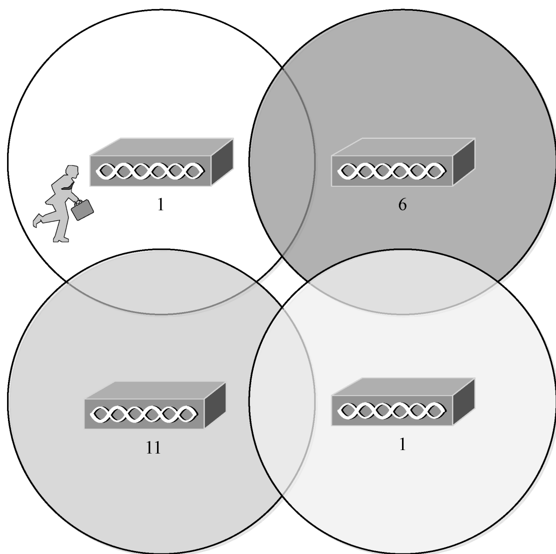


图 2-6　交替使用 IEEE 802.11b/g 信道时出现的空洞

相反，应像蜂巢那样对蜂窝进行布局，如图 2-7 所示，从而避免了干扰，在采用如图 2-7 所示的模式使用信道时，可以有多种不同的组合方式，但结果基本上相同。

注意，图 2-7 中显示，在使用信道 1 的蜂窝内的客户端移动时，将漫游到使用不同信道的相邻蜂窝中，为确保能够正常地漫游，客户端必须能够从一个信道切换到另一个信道，交替使用信道可避免重叠，这常被称为信道重用，可重复如图 2-7 所示的基本模式，以覆盖更大的区域，如图 2-8 所示。

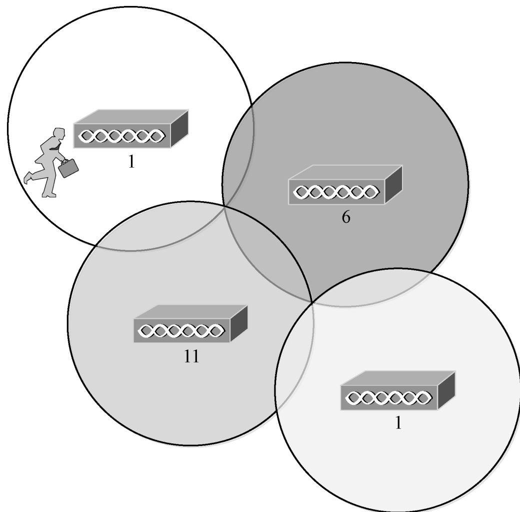


图 2-7　交替使用 IEEE 802. 11 b/g 信道的模式

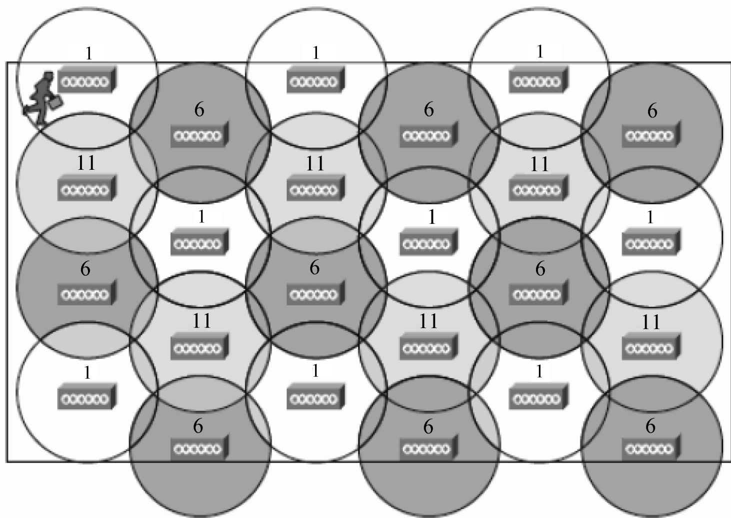


图 2-8　重复 IEEE 802 .11b/g 信道使用模式，以覆盖更大的区域

在 IEEE 802.11a 中，设计方案截然不同，它提供了 4、8 甚至 12 个互不重叠的信道，因此相邻蜂窝使用相同信道的可能性非常低。在美国，FCC 又增加了 11 个信道，总共有 23 个互不重叠的信道。

到目前为止，只讨论了二维区域的信道布局。例如，图 2-8 可能表示的是大楼一层楼面，如果需要设计一个覆盖大楼多层的无线局域网，情况又将如何呢？

前面介绍过，天线发射的 RF 信号实际上是在三维空间内传播的，对于全向天线，其辐射图是一个以天线为中心的圆环，信号向外传播，使得蜂窝在楼面上类似于一个圆，信号也将向下和向上传播（虽然传播距离没有水平传播那么远），这将影响位于相邻楼层中的 AP 蜂窝。

考虑一座三层大楼，如图 2-9 所示，在一楼使用的是图 2-8 所示的二维信道布局，在该图中，故意拉开了楼层之间的距离，以便能够看清使用的信道布局和信道号。实际上，相邻楼层中的蜂窝将相互重叠，就像同楼层的相邻蜂窝一样。

在这种情况下，在楼层平面内以及楼层之间都需要交替地使用信道。一楼的信道 1 不能与二楼和地下室的信道 1 相互重叠，在考虑设计和维护无线局域网所涉及的每项任务时，它们就像是要解决的难题，必须对每个 AP 的蜂窝大小、发射功率和使用的信道进行协调。如果要允许客户端跨越整个园区无线网进行漫游，漫游也将是一个问题。

好消息是，第 3 章（思科统一无线网络）讨论了如何解决这些众多的难题。

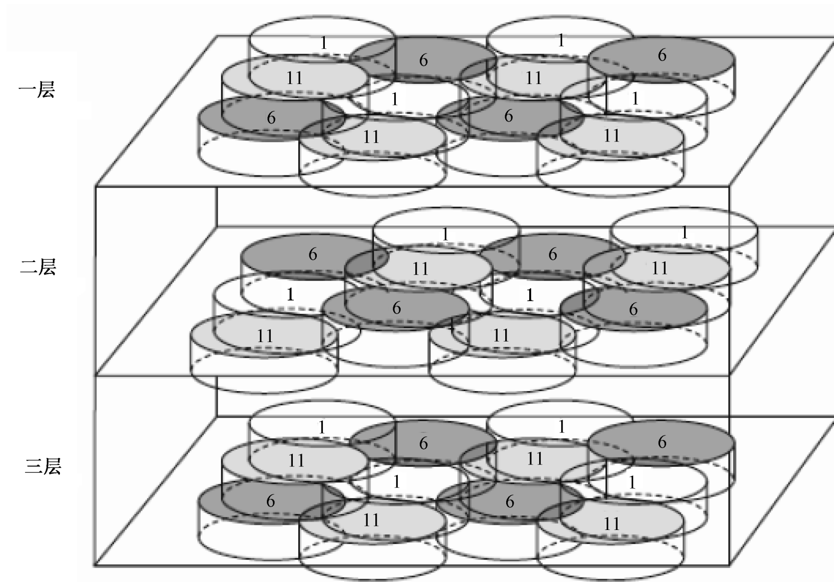


图 2-9　三维信道布局

2.4　用户设备选型

用户可向很多不同的厂商购买无线设备，它们的功能和需求各不相同。另外，无线客户端可以是计算机平台内置或外置的适配器，它们也可以嵌入到其他设备中，如手机、无绳电话、PDA、医疗设备和用于跟踪位置的标签，这些设备通常被称为特定应用设备（Application Specific Device，ASD）。

如果在网络中使用 Cisco AP，必须知道每台无线设备是否与打算使用的功能兼容。Cisco 开发了程序 Cisco Compatible Extensions（CCX）来满足这种需求，要确定设备是否是 CCX 兼容的，必须对其兼容性进行全面的测试和验证，在需要使用标准指定前的功能，而又无法确定各家厂商是否以相同方式实现了该功能时，这很方便。

随着时间的推移，不断有新的无线局域网功能推出，CCX 程序也在不断发展，以便能够测试这些功能，CCX 有不同的版本，高版本支持低版本支持的所有功能，最新的 CCX 版本为 5。表 2-2 介绍了各种 CCX 版本的基本功能组。

表 2-2　CCX 的功能

CCX 版本	包含的功能
CCXv1	基本的 IEEE 802.11 和 WiFi 兼容性 LEAP 802. 1X 认证，使用多个 SSID
CCXv2	WPA、PEAP 和 IEEE 802.1X 认证，使用 CCKM 实现快速漫游，用于 WLAN 现场勘查和干扰监控的 RF 扫描
CCXv3	WPA2，包括 AES 加密、EAP-FAST、IEEE 802. 1X 认证和 IEEE 802.11e QoS 标准中的 WiFi 多媒体（WMM）
CCXv4	Cisco 网络访问控制（NAC），IP 语音（VoIP）呼叫访问控制，报告 VoIP 度量值，增强的漫游，IEEE 802.1 位置标签功能（无线射频识别[RFID]）

第3章



思科统一无线网络

本章要点

- 思科统一无线网络架构
- 轻量级 AP 的关联和漫游

3.1　思科统一无线网络架构

在第 1 章和第 2 章中介绍过，无线局域网（WLAN）架构是以无线接入点（AP）为中心的，每个 AP 都是其 BSS 的中央枢纽，位于蜂窝内的客户端与之建立关联，前往和来自每个客户端的数据流必须通过 AP 才能到达网络的其他部分。

注意，虽然 AP 放在中央以支持客户端，但它是完全独立的，必须分别对每个 AP 进行配置，虽然很多 AP 配置的网络策略可能相同，但每个 AP 还必须独立地运行：AP 处理对无线射频（RF）信道的使用，客户端直接同 AP 关联，AP 独立地实施安全策略，等等。

简单地说，网络中的每个 AP 都是自主的，Cisco 将此称为自主模式 AP，以将其同更高级的模式区分开来。由于每个 AP 都是自主的，因此管理无线网络的安全性将非常困难，每个自主 AP 处理其安全策略，在无线网络和有线网络之间没有中央入口，这意味者没有合适的地方对数据流进行监控，以实现入侵检测和防范、服务质量及带宽控制等。

最后，管理众多自主 AP 的 RF 运行方式很困难，作为网络管理员，需要负责选择和配置 AP 信道，需要检测并确定可能带来干扰的恶意 AP，还必须管理 AP 的输出功率，确保无线覆盖范围足够大，同时重叠不大，且没有未被覆盖的地方——即使某个 AP 出现故障。

Cisco 意识到了自主 AP 的缺点，提供了一种更统一的方法，对于基于自主 AP 的 WLAN，我们应了解其一些重要的概念，以便能够对传统架构和将要介绍的统一架构进行比较。

3.1.1　传统的 WLAN 结构

首先，来看一下自主 AP 架构中的数据流模式，在图 2-1 中，两个客户端关联到一个自主 AP，所有前往和来自客户端的数据流都必须经过 AP，从客户端 A 前往网络部分的数据流将经过 AP 并在这里被桥接到交换型网络，即使是两个无线客户端之间的数据流也不能直接传输，而必须首先通过 AP，然后前往另一个客户端。

第 2 章介绍过，AP 可支持多个服务集标识符（SSID），这就要求多个 VLAN 通过中断链路扩展到该服务集中。如果要让多个自主 AP 使用相同的 SSID，VLAN 必须以连续方式扩展到这些 AP，这意味着交换型网络必须将 VLAN 传输到每个需要它们的 AP，如图 3-1 所示。

在图 3-1 中，两个 AP 都使用 SSID A 和 SSID B，这两个 SSID 分别对应于 VLAN A 和 VLAN B，两个 AP 必须连接到同一个交换型网络，后者需要在第二层扩展 VLAN A 和 VLAN B，这是通过使用连接到每个 AP 的 IEEE 802.1q 中继链路来传输 VLAN A 和 VLAN B 的数据流来实现的。

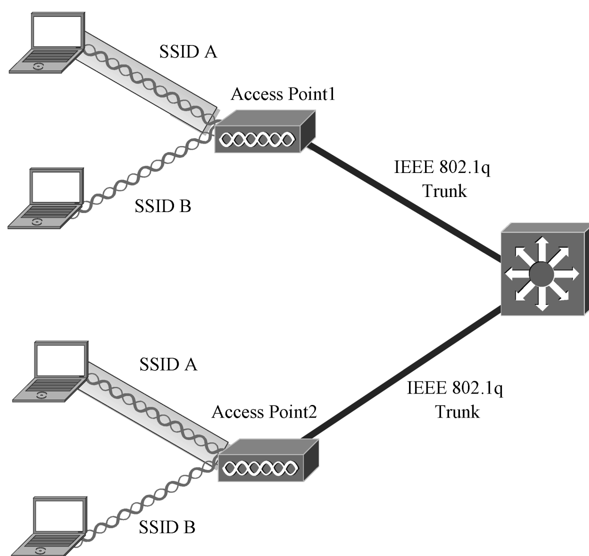


图 3-1　覆盖多个自主 AP 的 VLAN

由于 SSID 及其 VLAN 必须在第二层进行扩展，因此必须考虑它们是如何扩展到整个交换型网络的。在图 3-1 中，SSID A 和 VLAN A 覆盖的范围用阴影表示，显然，它们形成了一个覆盖了两个 AP 的连续路径，这样无线客户端始终能够使用 SSID A。

当需要在大型网络中的众多 AP 中使用相同的 SSID，以便无线客户端能够漫游到区域内的任何地方时，该 SSID 及其 VLAN 必须扩展到用户可能漫游到的所有地方，这将导致需要建立覆盖整个园区网的 VLAN，这有悖于思科倡导的良好网络设计实践。

3.1.2　Cisco 统一无线网络的组成

Cisco 收集了无线局域网不可或缺的一整套功能，将其称为 Cisco 统一无线网络，这种新架构提供了下述功能，它们被集中在一起，以便能够影响位于网络中的所有无线局域网设备：

- WLAN 安全；
- WLAN 部署；
- WLAN 管理；
- WLAN 控制。

为集中 WLAN 的这些功能，将自主 AP 的很多功能移到了一个中央位置，图 3-2 的上半部分列出了自主 AP 执行的大部分功能，它们分成两组，位于左边的实时进程和位于右边的管理进程。

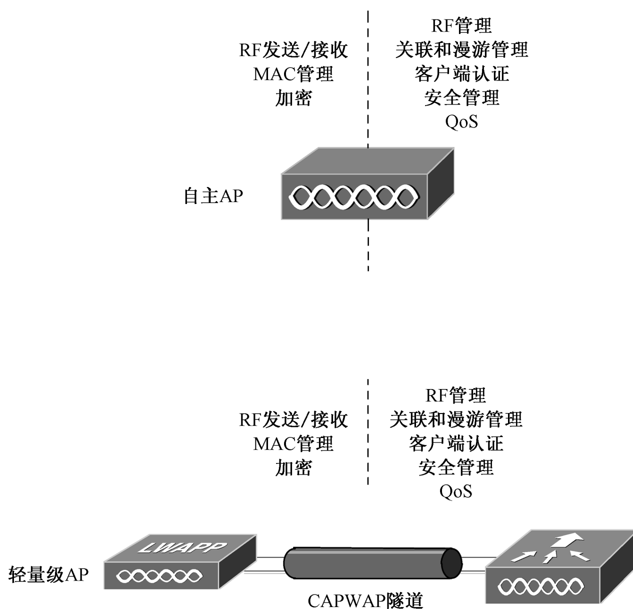


图 3-2　自主 AP 和轻量级 AP 的比较

实时进程包括发送和接收 IEEE 802.11 帧、AP 信标和探针消息，数据加密也是以实时方式对每个分组进行的，AP 必须在介质访问（MAC）层同无线客户端交互，这些功能必须在离客户端最近的 AP 硬件中完成。

管理功能并非是 RF 信道发送和接收帧的有机组成部分，而应集中进行管理，因此，这些功能被移到一个远离 AP 的中央平台中。

在 Cisco 统一无线网络中，轻量级接入点（LAP）只执行实时的 IEEE 802.11 操作，之所以将其称为 LAP，是因为它除去了代码映像和本地智能，相对于传统自主 AP 来说是轻量级的。

管理功能都由无线局域网控制器（WLC）执行，WLC 由众多 LAP 所共享，如图 3-3 的下半部分所示。注意，LAP 只执行第一和二层的功能，帧在这两层进入或离开 RF 域，LAP 完全依赖于 WLC 来执行其他 WLAN 功能，如用户认证、安全策略管理以及 RF 信道和输出功率的选择。

这种分工被称为 Split-MAC 架构，在这种架构中，正常的 MAC 操作被分为两个不同的地方，网络中的每个 LAP 都如此，它们必须将自己绑定到一个 WLC 才能启动并支持无线客户端，WLC 成为中央枢纽，支持分散在交换型网络中的大量 LAP。

LAP 如何绑定到 WLC 以成为正常运行的完整接入点呢？必须在这两种设备之间建立一条隧道，用于传输与 IEEE 802.11 相关的消息和客户端数据，LAP 和 WLC 可以位于同一个 VLAN 或 IP 子网中，但并非必须如此；相反，它们可以位于两个完全不同的 IP 子网中，而这两个 IP 于网可以位于不同的地方。之所以可行，是因为隧道将 LAP 和 WLC 之间传输的数据封装到 IP

分组中，从而可以跨越园区网交换或路由这些数据，图 3-3 说明了这个概念。

LAP 和 WLC 使用无线接入点控制和配置协议（CAPWAP 协议，Control And Provisioning of Wireless Access Points，早期版本叫轻量级接入点协议，LWAPP）作为隧道化协议。实际上，Control And Provisioning of Wireless Access Points 由两个隧道组成，分别为控制信息隧道和数据隧道，如图 3-4 所示。

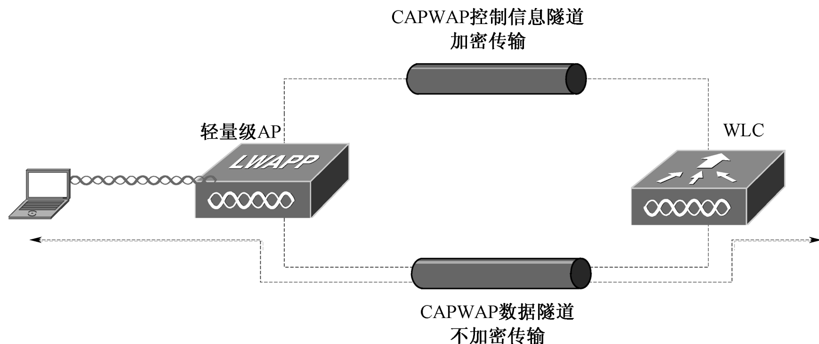


图 3-3 使用 CAPWAP 连接 LAP 和 WLC

CAPWAP 控制消息隧道用于配置 LAP 和管理其运行方式，对控制消息进行认证和加密，确保 WLC 能够可靠控制 LAP，控制信息隧道主要实现如下的功能：

- AP 通过控制消息隧道发现 WLC；
- 在 AP 和 WLC 之间建立相互信任；
- AP 使用控制消息隧道下载固件；
- AP 使用控制消息隧道下载配置文件；
- WLC 收集 AP 的各项统计数据；
- 移动和漫游相关的任务；
- AP 发送给 WLC 的通知及警告信息；
- 其他一些任务。

CAPWAP 的数据隧道用来封装前往和来自与 LAP 相关联的无线客户端的数据，但没有进行加密。

CAPWAP 在 WLC 端使用 UDP 目标端口 5246 和 5247（原先的 LWAPP 在 WLC 端使用 UDP 目标端口 12222 和 12223）。

LAP 和 WLC 必须使用数字证书彼此认证对方，出厂时每台设备都预安装了一个 X.509 证书，通过在幕后使用数字证书，可以在每台设备成为 Cisco 统一无线网络的一部分前正确地对其进行认证，这有助于确保恶意 LAP 和 WLC（冒充的 LAP 或 WLC 设备）无法进入网络。

3.1.3　WLC 功能

在 WLC 和一个或多个轻量级 AP 之间建立 CAPWAP 隧道后，WLC 便能够提供各种其他功能。下述是 WLC 功能列表，阅读时请回想一下前面讨论过的传统 WLAN 架构面临的困扰和缺点。

① 动态地分配信道：WLC 根据区域内其他活动的接入点，为每个 LAP 选择并配置 RF 信道。

② 优化发射功率：WLC 根据所需的覆盖范围设置每个 LAP 的发射功率，发射功率还将定期地自动调整。

③ 自我修复无线覆盖范围：如果某个 LAP 出现故障，将自动调高周围 LAP 的发射功率，以覆盖出现的空洞。

④ 灵活的客户端漫游：客户端可在第二层或第三层漫游，且切换时间非常短。

⑤ 动态的客户端负载均衡：如果多个 LAP 覆盖的地理区域相同，WLC 将让客户端同用户最少的 LAP 相关联，从而在 LAP 之间分配客户端负载。

⑥ RF 监控：WLC 负责管理每个 LAP，因此能够通过扫描信道来监控 RF 的使用情况，通过侦听信道，WLC 能够远程收集有关 RF 干扰、噪声、周围 LAP 发出的信号以及恶意 AP 或特殊客户端发出的信号。

⑦ 安全性管理：在允许无线客户端关联并接入 WLAN 前，WLC 可以要求它们从可信的 DHCP 服务器那里获得 IP 地址，同时通过第二层或第三层的网络认证。

很多平台都支持 Cisco WLC，主要差别在于管理的 LAP 数量。表 3-1 列出了支持 Cisco WLC 的平台及其功能。

表 3-1　支持 Cisco WLC 的平台及其功能

型　　号	接　　口	属　　性
2006	4 个 10/ 100TX	最多可处理 6 个 LAP
2106	8 个 10/100TX，其中 2 个 PoE 端口	最多可处理 6，12，25 个 LAP
2504	4 个 GigE，其中 2 个 PoE 端口	最多可处理 5～50 个 AP，是 2006 及 2106 的升级产品
4402	2 个 GigE	最多可处理 12、25 或 50 个 LAP
4404	4 个 GigE	最多可处理 100 个 LAP
WiSM	不适用（集成在 Catalyst6500 中）	包含两个 WLC 4404 的 Catalyst 6500 模块，最多可处理 300 个 LAP（每个 4404 控制器 150 个），在单个机架中最多可置装 5 个 WiSM（在最新的 4.2 版本中支持单个机架最多安装 6 个 WiSM）
WiSM2	不适用（集成在 Catalyst6500 中）	是 WiSM 的升级产品，同 WiSM 不同之处在于内部只有一个控制器，最多可处理 1 000 个 AP，采用 10 Gbps 的速度同背板连接

续表

型　　号	接　　口	属　　性
5508	8 个 SFP GigE	根据不同的型号可支持 12, 25, 50,100, 250 最多 500 个 AP，7 000 个用户，是 4400 系列的升级产品
用于 ISR 路由器的 WLC 模块	可集成到 2800、3700 和 3800 路由器中	最多可处理 6、8 或 12 个 LAP
集成了 WLC 的 Catalyst 3750G	不适用（集成在交换机中）	每台交换机最多可处理 25 或 50 个 LAP，每个交换机堆栈最多可支持 100 个 LAP
8500	2 个 TenGig	每个支持最多 6 000 个 AP，吞吐量 10 Gbps

在网络中可以部署多个 WLC 以处理大量的 LAP，另外，使用多个 WLC 提供了一定的冗余性，当某个 WLC 出现故障时 LAP 将能够恢复。

管理多个 WLC 将消耗大量的精力，因为需要管理和监控的 LAP 很多。Cisco 无线控制系统（Wireless Control System, WCS）是一个可选的服务器平台，可作为网络中所有 WLC 的 GUI 前端。在 WCS 中，可以执行任何 WLAN 管理和配置任务，还可以规划 RF 和跟踪无线用户。

WCS 使用楼面布置图来动态地显示无线覆盖范围，还可以将有关大楼的建造信息提供给它，使其能够更深入地了解 RF 信号的传播情况。这样做后，WCS 就能根据多个收到客户端信号的 LAP 决定客户端的位置，其误差在几米之内。

WCS 还能够同 Cisco 无线定位装置（Wireless Location Appliance）协同工作，以跟踪数千个无线客户端的位置，甚至可以使用 IEEE 802.11 RFID 有源标签，以跟踪物体在无线覆盖区域内的位置，在需要找出恶意的无线客户端或需要跟踪在大楼内移动的公司财产时，使用 MAC 地址来跟踪物体将很方便。

3.1.4　轻量级 AP 的工作原理

LAP 被设计为无须接触它就能对其进行配置，LAP 必须找到一个 WLC 并获得所有的配置参数，因此无须通过控制台端口或网络对其进行配置。

下面的步骤详细描述了 LAP 进入活动状态之前必须完成的启动过程。

- 第 1 步：LAP 从 DHCP 服务器那里获得一个 IP 地址。
- 第 2 步：LAP 获悉所有可用 WLC 的 IP 地址。
- 第 3 步：LAP 向其地址列表中的第一个 WLC 发送加入请求消息，如果该 WLC 没有应答，将尝试下一个 WLC；当 WLC 接受 LAP 时，将向 LAP 发回加入响应消息，这将把两台设备绑定起来。
- 第 4 步：WLC 将 LAP 的代码映像版本同本地存储的代码映像版本进行比较，如果不同，LAP 将下载 WLC 存储的代码映像并重新启动。
- 第 5 步：WLC 和 LAP 建立一条加密的 CAPWAP 隧道和一条不加密的 CAPWAP 隧道，

前者用于传输管理数据流，而后者用于传输无线客户端的数据。

在上述步骤中，我们应注意到两点，在第 2 步中，LAP 可以使用下述任何方法来查找 WLC 的 IP 地址（详细查找过程见附录描述）。

① DHCP 服务器：它在包含 WLC 地址列表的应答中添加选项 43。

② LAP 使用 IP 子网广播地址广播一条加入请求消息，希望有 WLC 也连接到该子网或 VLAN 中，仅当 LAP 和 WLC 在第二层相邻时，这种方法才管用。

③ 在任何时刻，LAP 总是加入或关联到一个 WLC，然而，LAP 能够维护一个最多可包含 3 个 WLC（主 WLC、辅助 WLC 和第 3 WLC）的列表。当 LAP 启动时，它按顺序同每个 WLC 联系，如果找不到做出响应的 WLC，LAP 将尝试使用 IP 子网广播来找到可用的 WLC。

④ 当 LAP 启动并成功地加入一个 WLC 后，如果该 WLC 由于某种原因出现故障，LAP 将无法继续转发数据流和维护客户端关联。因此，LAP 在意识到其 WLC 没有响应后，它将重新启动并搜索处于活动状态的 WLC，这意味着在 LAP 重新启动并加入其他控制器期间，所有客户端关联都将终止。

⑤ 在 LAP 断开同 WLC 的联系后，客户端关联通常会终止，客户端无法通过 WLAN 传输数据，一个特例是用于远程场点的 Cisco 远程边缘接入点（Remote Edge Access Point, REAP）。在远程场点中，LAP 通过 WAN 链路连接 WLC。当使用 REAP 时，即使 WAN 链路出现故障导致 WLC 不可用，LAP 仍能够继续运行，这让无线用户能够继续在远程场点内通信，直到链路和 WLC 恢复正常。

3.1.5 思科统一无线网络中的数据流格式

由于轻量级 AP 通过逻辑 CAPWAP 隧道连接到交换型网络，因此进入和离开 WLAN 的数据流模式不同于传统 WLAN。

请看图 3-4 所示的网络，两个无线客户端关联到由 LAP 和 WLC 组成的 WLAN。从客户端 A 出发前往网络其他地方的数据流将经过 LAP 和连接到 WLC 的 CAPWAP 隧道，然后进入交换型园区网。

然而，对于两个无线客户端之间的数据流，其传输路径很有趣，这种数据流从客户端 A 出发，经 LAP 和 CAPWAP 隧道进入 WLC，然后经 CAPWAP 隧道和 LAP 到达客户端 B，这进一步说明 WLC 在统一无线网络架构中扮演了至关重要的角色。

虽然进入和离开 WLAN 的数据流都必须经过 CAPWAP 隧道和 WLC，但并非所有数据流操作都是在隧道两端进行的。

例如，可以使用无线加密来确保数据通过空气传播时的安全，就像传统 WLAN 一样，然而，加密后的数据根本不会通过 CAPWAP 隧道，分组在离开无线客户端时被加密，并在到达 LAP 后被解密，分组认证（如果使用的话）也是如此。

所有分组认证和加密功能都是由 LAP 硬件完成的，而没有将其移到 WLC 中。

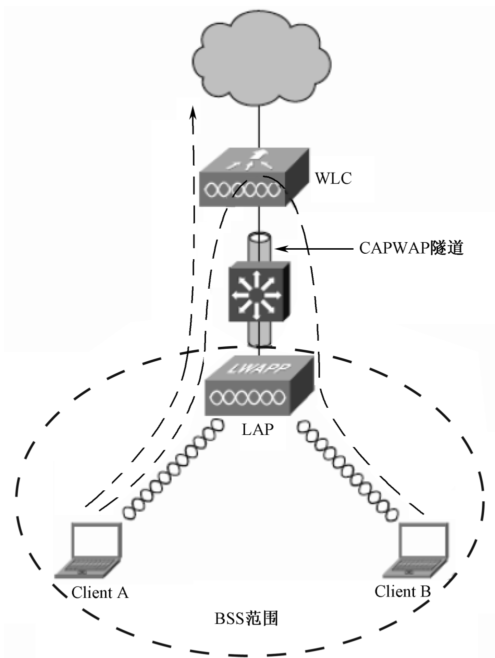


图 3-4　使用轻量级 AP 时的数据流模式

在网络中使用自主 AP 时，必须将为无线客户端提供服务的 VLAN 进行扩展，使其覆盖 AP，而使用轻量级 AP 时，不需要这样做。

首先，来看如图 3-5 所示的示例网络，两个 VLAN（A 和 B）用于传输无线客户端数据流，它们分别被关联到 SSID A 和 SSID B。注意：VLAN A 和 VLAN B 只延伸到交换机 SW2 和 WLC 之间的中继链路上；另外，WLC 和 LAP 是通过 IP 网络连接起来的，同接入 VLAN A 和 VLAN B 无任何联系。

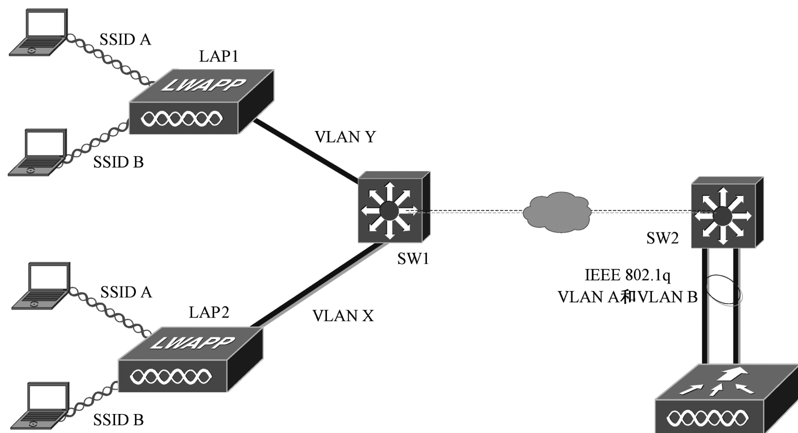


图 3-5　支持多个 VLAN 和 SSID 的统一无线网络

加入 VLAN 的数据流实际上是通过 CAPWAP 隧道传输的，因此从逻辑上说，它们覆盖了用户所在的 LAP，图 3-6 说明了这一点，其中 VLAN A 扩展到了两个 LAP，并在这里被映射到 SSID A。

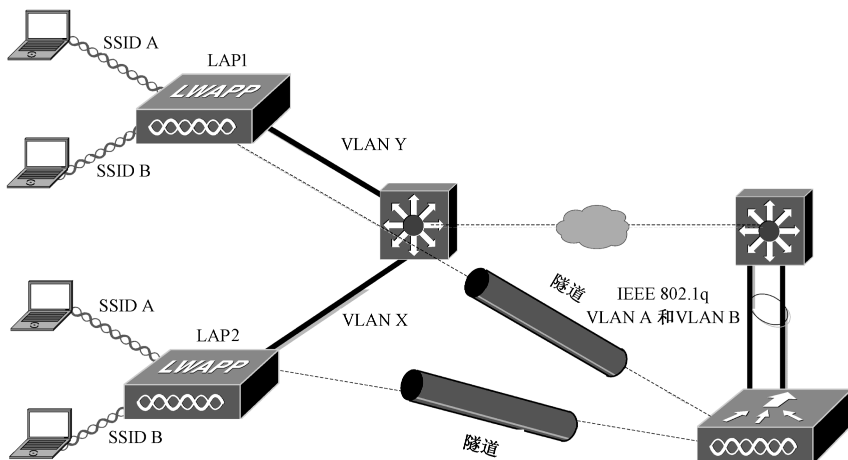


图 3-6　通过 CAPWAP 隧道扩展的 VLAN A

3.2　轻量级 AP 的关联和漫游

无线客户端必须同轻量级 AP 协商关联，这与所有 IEEE 802.11 无线网络一样。然而，Split MAC 架构对客户端管理有一个有趣的影响，因为 LAP 只负责完成实时无线功能，因此它将客户端的关联请求传递给 WLC，也就是说，无线客户端直接同 WLC 协商关联，其原因有两个：

- 可以在一个中央位置管理所有的客户端关联；
- 客户端漫游更快、更容易，因为直接在控制器中维护或解除关联。

当使用自主 AP 时，客户端通过将关联从一个 AP 切换到另一个 AP 来实现漫游，客户端必须分别同每个 AP 进行协商，而在切换关联时，前一个 AP 必须将来自客户端的缓存数据交给下一个 AP；当使用自主 AP 时，漫游只发生在第二层，要支持第三层漫游，必须采取其他措施。

在使用轻量级 AP 时，客户端也是通过切换关联来进行漫游的，在客户端看来，关联是在 AP 之间切换的，但实际上是根据 AP-WLC 绑定在 WLC 之间切换的。

通过 WLC 的帮助，轻量级 AP 可以支持第二层和第三层漫游，客户端关联且总是对应一条 CAPWAP 隧道，当切换到新的 AP 时，关联也将对应到新的隧道，即将新 AP 连接到的 WLC 的隧道。

漫游时，客户端的 IP 地址可保持不变，而不管客户端通过哪条 CAPWAP 隧道连接到控制器。接下来的几小节将从负责管理漫游和客户端关联的 WLC 的角度讨论客户端漫游。

3.2.1 控制器内漫游

在图 3-7 中，一个无线客户端在位置 A 时有活动的无线关联，这是通过 AP1 关联 WLC1 的，正如您预期的，所有前往和来自该客户端的数据流都将通过 AP1 和 WLC1 之间的 CAPWAP 隧道。

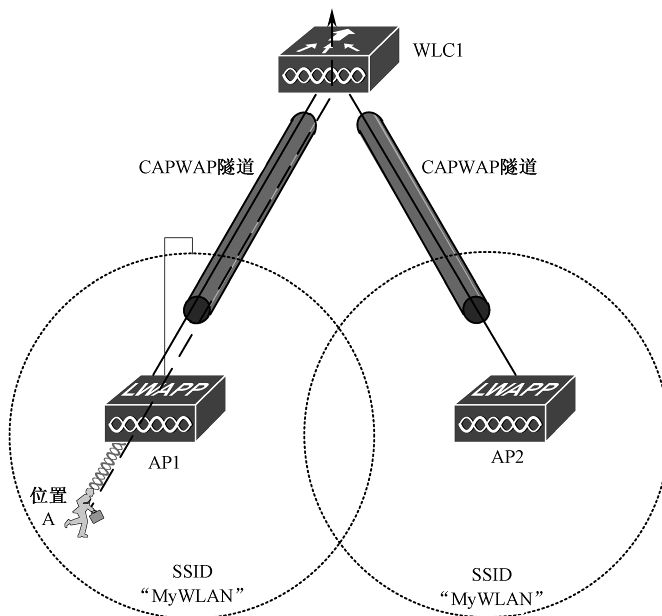


图 3-7 漫游前位于 LAP 1 蜂窝内的无线客户端

在图 3-8 中，客户端开始移动，漫游到 AP2 覆盖的区域内，就这个例子而言，有两点需要注意：AP1 和 AP2 提供的蜂窝都使用 SSID“MyWLAN”，这让客户端能够在它们之间漫游；AP1 和 AP2 连接到的是同一个控制器 WLC1。

在图 3-8 中，客户端变成了通过 AP2 关联到 WLC1，虽然使用的 AP 不同，但关联和 CAPWAP 隧道是由同一个控制器提供的，这被称为控制器内漫游，客户端的关联仍在同一个控制器内。

这种漫游很简单，因为控制器 WLC1 只须更新其列表，以便使用连接到 AP2 的 CAPWAP 隧道来找到客户端即可，在控制器内，很容易将为旧关联缓存的数据移交给新关联。

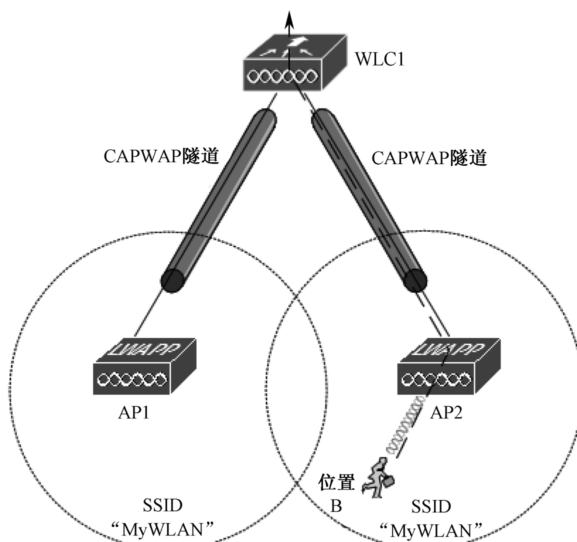


图 3-8　漫游到新的 LAP2 蜂窝内的无线客户端

3.2.2　控制器间漫游

在有些情况下，客户端可能从一个控制器漫游到另一个控制器。例如，大型无线网络可能包含大量 LAP，使用单个 WLC 无法支持它们，也可能为实现负载均衡和冗余而将 LAP 分散到多个控制器。

在图 3-9 中，无线客户端当前通过 AP1 关联到 WLC1，这类似于图 3-8，但两个相邻的 LAP 蜂窝属于不同的 WLC。所有客户端的数据流都将经过 AP1 传送到 WLC1 的 CAPWAP 隧道。

当客户端移动到 AP2 的蜂窝内时，发现使用的 SSID 相同，因此客户端可以将关联切换到 WLC2，只要两个控制器（WLC1 和 WLC2）位于同一个 IP 子网中，它们就能轻松地交接客户端的关联。这是通过移动消息交换将有关客户端的信息从一个 WLC 传给另一个 WLC 实现的，如图 3-10 所示。

当完成移动消息交换后，客户端便将使用 AP2 和 WLC2 之间 CAPWAP 隧道。客户端的 IP 地址没变，实际上，漫游过程对客户端来说是完全透明的。

下面来看图 3-11 所示的情形，两个控制器 WLC1 和 WLC2 位于不同的 IP 子网中，这两个子网分别是 VLAN A 和 VLAN B。一开始，无线客户端位于 AP1 蜂窝中，并关联到 WLC1。客户端获得的 IP 地址位于 VLAN A 中，因为 AP1 将 VLAN A 映射到其 SSID，该客户端的所有数据流都将通过 AP1 和 WLC1 之间的 CAPWAP 隧道传输到 VLAN A 中。

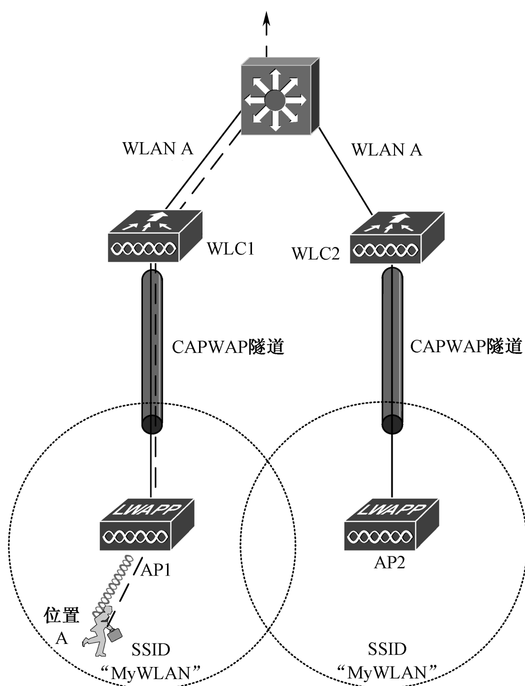


图 3-9　漫游到其他控制器前的无线客户端

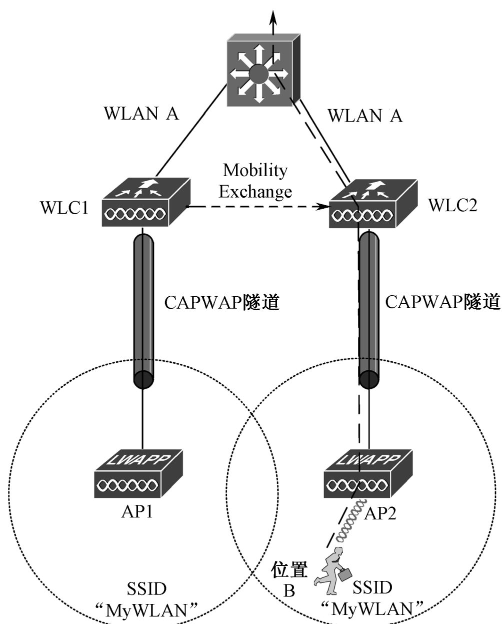


图 3-10　进行控制器漫游后（控制器位于同一子网）

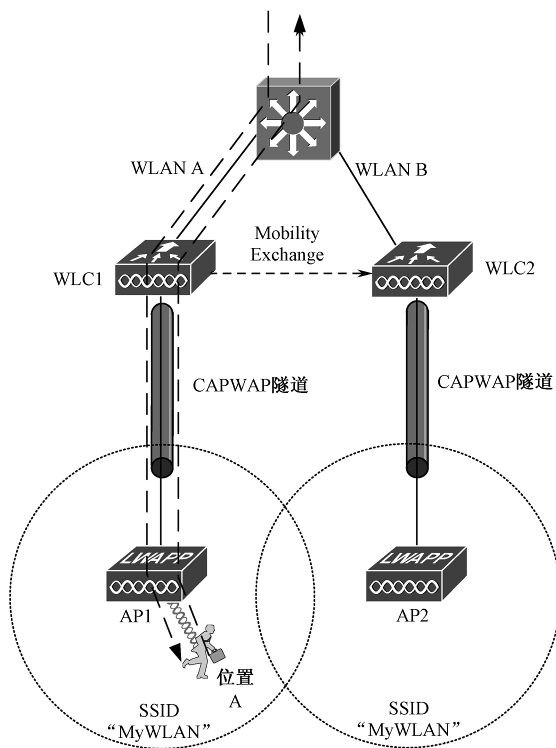


图 3-11　发生控制器间漫游前（控制器位于不同的子网中）

当客户端移动到 AP2 提供的蜂窝内后，将发生一些有趣的事情。在图 3-12 中，客户端通过 AP2 关联到 WLC2，后者让客户端能够接入 VLAN B，客户端的 IP 地址没变，但由于 WLC1 和 WLC2 位于不同的子网（VLAN）中，因此客户端的 IP 地址移到了其他子网内，两个控制器必须协同工作，以便继续为客户端提供服务，而不要求客户端获得新的 IP 地址，两个控制器在它们之间建立一条 Ether-IP 隧道，用于传输前往客户端的数据流。通过使用 Ether-IP 隧道，控制器可以使用 IP 协议 97 将 MAC 层数据封装在 IP 分组中，为将分组转发给客户端，一个控制器封装分组并将其发送给另一个控制器，后者通过隧道收到分组后将其拆封，使其格式与原来相同（Ether-IP 隧道是在 RFC 3378 中定义的）。

并非客户端的所有数据流经过的路径都相同，离开客户端的数据流经 CAPWAP 隧道从 AP2 传输到 WLC2，然后进入 VLAN B，这可能与您预期的相同。虽然客户端的 IP 地址并不属于新的 VLAN，但仍可以将分组发送到该 VLAN。

前往客户端的数据流采用不同的路径，在图 3-12 中，数据流经交换机进 VLAN A，然后被转发到 WLC1，这些数据流为何进入 VLAN A 而不是客户端现在位于的 VLAN B 呢?因为客户端使用的 IP 地址属于 WLAN A，因此它仍属于 VLAN A，而不管它漫游到无线网络的什么地方。前往该客户端的数据流的目标地址位于 WLAN A 中，必须将其转发到 VLAN A，因此，

WLC1 必须接收这种数据流，并将其转发到客户端当前关联的控制器，WLC1 通过 Ether-IP 隧道将数据流转发给 WLC2，后者再通过连接到 AP2 的 CAPWAP 隧道将数据流转发给客户端。

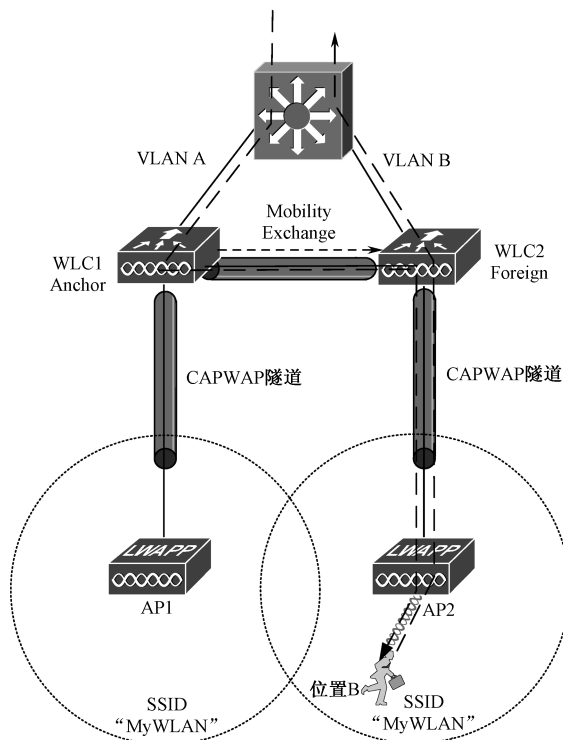


图 3-12　发生控制器间漫游后（控制器位于不同的子网中）

由于客户端最初是通过 WLC1 加入到 WLAN 中的，因此 WLC1 始终是该客户端的锚点（Anchor Point），为其他子网中的客户端提供服务的控制器被称为外部代理（Foreign Agent）。当客户端漫游时，锚点 WLC 将做出相应的反应，通过 Ether-IP 隧道连接到客户端当前外部代理 WLC，我们称这种漫游机制为非对称漫游。当然思科也支持对称方式的漫游机制，即离开客户端的数据流和前往客户端的数据流采用相同的路径，均通过 Ether-IP 隧道从锚点 WLC 进出。

3.2.3　移动组

要进行控制器间漫游，客户端必须能够在与不同控制器关联的 LAP 之间漫游。在漫游期间，控制器之间必须能够交换客户端的关联信息。为此，将 WLC 组合成逻辑移动组，客户端可漫游到任何 LAP（及其关联的 WLC），只要后者位于同一个移动组中，一个移动组最多可包含 24 个不同类型和平台的 WLC，移动组包含的 LAP 数量随 WLC 管理的 LAP 数量而异，而

后者又随平台而异。

有时候，无线客户端在移动时可能跨越移动组边界，两个相邻 LAP 属于不同的移动组。在这种情况下，客户端可将其关联切换到新的移动组中，但其 IP 地址及 WLC 维护的全部信息都将被丢弃。

多个 WLC 的设备可以被配置成一个移动组，移动组允许在一个网络内部署多个 WLC 并在它们之间动态地共享重要的数据。当控制器间出现漫游时，移动组可以用来转发数据。共享的信息包括客户端设备的上下文状态以及 WLC 的负载状况。有了这些信息以后，网络能够轻易地支持控制器间的漫游、AP 的负载均衡以及控制器的冗余，图 3-13 显示了移动组的概念。

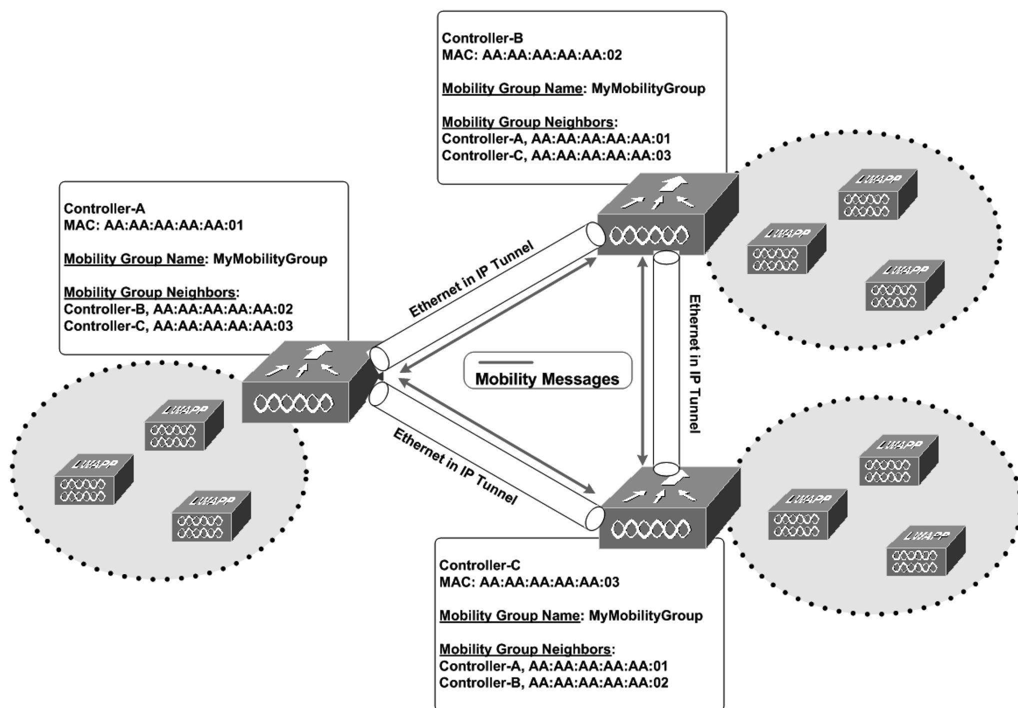


图 3-13　移动组示意图

从图 3-13 中可以看出，移动组中的每一个 WLC 都配置了一串移动组中其他成员的信息。每个 WLC 同组中其他 WLC 创建了一个邻接关系，如果客户数据在移动组的成员之间转发以支持第三层漫游，这些数据包将被封装在 Ether-IP 的隧道中。

一个移动组最多可以包含 24 个不同种类的 WLC，组中的 AP 数量因 WLC 支持的 AP 数量不一，例如，24 个 WLC 如果都是 4404 控制器，则最多可以支持 24×100=2 400 个 AP；如果都是 WiSM 模块，则最多可以支持 150×24=3 600 个 AP；如果为 5508-500 型控制器，最多可支持 500×24=12 000 个 AP。

通常情况下，为了支持全网移动漫游，所有的 WLC 需要共享同一个移动组信息，如果确定没有漫游存在，也就没有必要将所有的 WLC 放置于同一个移动组中。例如，假设我们在两幢不同的楼内分别部署了一个 WLC 用来管理本楼内的 AP，如果两幢楼之间隔着一个操场，同时操场上又没有无线信号覆盖，不可能存在客户端从一幢楼漫游到另一幢楼的可能性，也就没有必要将这两个 WLC 放置于同一个移动组中。

冗余的 WLC 必须被配置在同一个移动组内，当一个 LAP 加入到 WLC 时，它从移动组中获得组中其他 WLC 的信息，这些地址将会被 LAP 存储起来待下一次 CAPWAP 发现时使用。

配置移动组需要如下的一些基本条件：

① 所有的 WLC 的 management 端口必须互连互通。

② 所有的 WLC 必须配置成使用同一个移动组名称，移动组名称区分大小写。

③ 移动组中的 WLC 必须使用同一个虚拟的接口地址。

④ 每个 WLC 中都必须配置组中其他 WLC 的 MAC 地址以及 IP 地址。

⑤ 每个 WLC 之间保证 UDP 端口 16666 和端口 16667 畅通，其中，端口 16666 用来传输移动组之间的控制信息，端口 16667 用来传输移动组之间 IPSec 的用户加密数据。

3.2.4 静态 IP 漫游

通常情况下，可移动客户端的 IP 地址都从 DHCP 服务器获得动态 IP 地址，如果一个用户开机并同某个 SSID 关联（或从没有同任何 AP 关联的状态到同某个 AP 上的 SSID 相关联），用户将获得此 SSID 对应的 WLAN 分配的 IP 地址，并建立网络连接。如果有些用户采用静态 IP 地址，在早期版本的 WLC 软件中，用户除非同自己 IP 子网具有相同地址段的 SSID 关联，否则将无法获得移动服务。在最新的 WLC 版本中，Cisco 已经提供了对静态 IP 地址的漫游支持。

具体描述如下：

① 当一个静态地址的用户同 WLC *x* 相关联后，但此 WLC *x* 不支持此 IP 地址子网段。

② 如果存在 L2 认证，在用户成功认证后，WLC *x* 将获知用户的 IP 地址信息。

③ WLC *x* 知道本地不存在这个 IP 子网，将会在移动组中的各 WLC 中询问是否有支持此 IP 子网的 WLC，如果有 WLC *y* 做出应答，WLC *x* 将会向 WLC *y* 发送一个锚（Anchor）请求，完成用户在 WLC *x* 与 WLC *y* 之间的漫游切换并建立一个从 WLC *x* 到 WLC *y* 的隧道。

图 3-14 显示了某个同 WLC1 关联的用户静态配置了 VLAN *X* 的 IP 地址，用户离开与之关联的 AP 的覆盖范围，并成功与 LAP1 解除关联，此用户后来进入 LAP2 的覆盖范围，并成功同 LAP2 相关联，由于与 LAP2 关联的 WLC2 上仅支持 VLAN Z 的地址段，WLC2 通过查找移动组中的配置信息，向移动组中的每个 WLC 发送查询信息，一但有 WLC 反馈，WLC2 将会向反馈的 WLC（本例中为 WlC1）发送一个锚请求，建立一个同 WLC1 的加密隧道，以后所有来往于静态地址用户的数据将借助加密隧道通过锚 WLC 传送到相应的接入子网（VLAN *X*）。

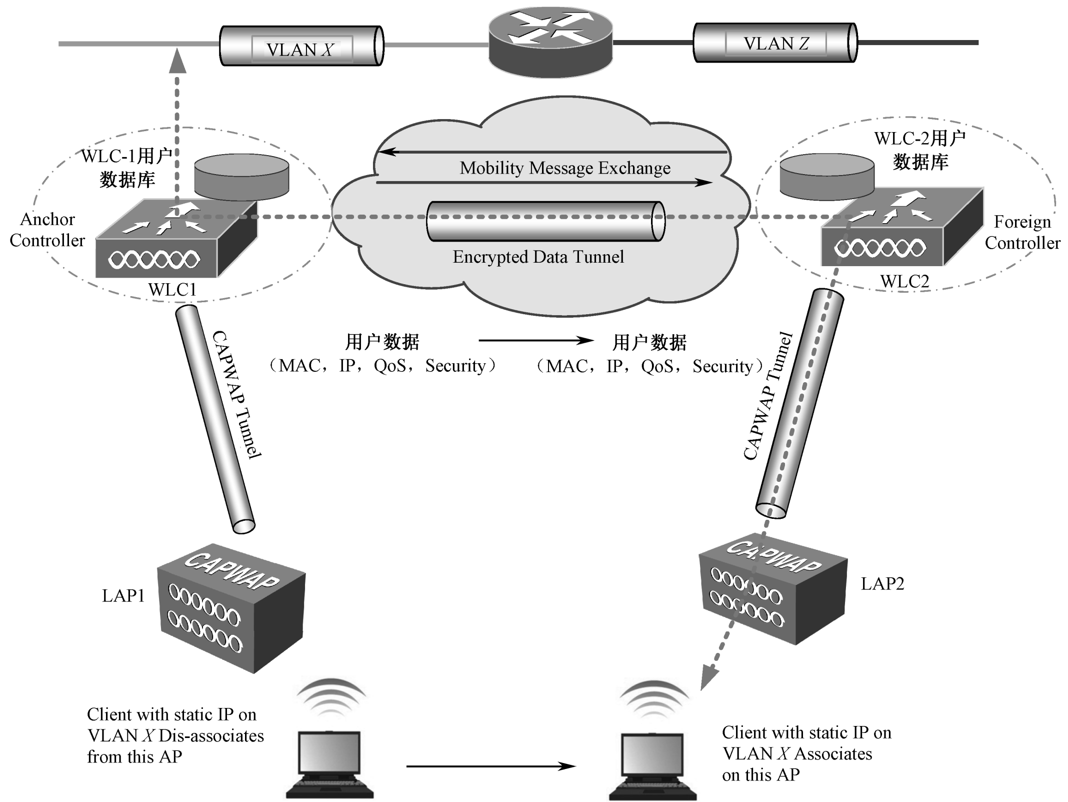


图 3-14　静态 IP 地址移动漫游

第4章 

思科统一无线局域网的配置

本章要点

- WLC 的基本配置
- 配置 HREAP
- 管理无线射频资源
- 配置 IEEE 802.11n 网络
- 配置 Cisco Wireless Mesh 网络
- 配置 LAP
- 控制器冗余及 LAP 的负载均衡
- 管理非法 AP
- 总结

本章详细介绍了一些简单的无线局域网控制器（WLC）和轻量级接入点的配置步骤，读者应熟悉在每种设备中输入初始配置的过程。

4.1 WLC 的基本配置

4.1.1 WLC 的组成及接口

Cisco WLC 有多种用于不同用途的接口，在配置 WLC 时，最难的部分可能是确定如何布局和连接接口。无论硬件型号如何，WLC 都包含下述接口类型，请参阅图 4-1，它描述了常用的接口。

（1）管理接口

管理接口是使用静态 IP 地址的接口，用于传输带内管理数据流，这些接口用于建立到 WLC 的 Web、安全外壳（SSH）或 Telnet 会话。

（2）AP 管理接口

AP 管理接口是使用静态 IP 地址的接口，所有 LAP 都使用它来端接 CAPWAP 隧道，WLC 也在该接口上侦听 LAP 在试图发现控制器时发送的子网广播。7.3 及以后版本，可以不配置 AP 管理接口，管理接口担任了 AP 管理接口的角色。

（3）虚拟接口

虚拟接口是用于中继来自无线客户端的 DHCP 请求的逻辑接口，给该接口分配一个伪造（但唯一）的静态 IP 地址，这样客户端将把该虚拟地址视为其 DHCP 服务器；在同一个移动组中，所有 WLC 都必须使用相同的虚拟接口地址。

（4）服务端口

服务端口是 Cisco 5500 系列 WLC 使用的带外以太网接口，仅当控制器正在启动或网络问题导致无法进行其他方式的接入时才使用它，Catalyst 6500 无线服务模块（Wireless Service Module，WiSM）有一个连接到机架监控器的内部服务端口。

（5）集散系统端口

集散系统端口是将 WLC 连接到园区网中交换机的接口，该接口通常是一个中继链路，用于传输覆盖了 LAP 和 VLAN 的数据流。

（6）动态接口

动态接口是根据需要为通过 CAPWAP 隧道扩展到 LAP 的 VLAN 自动创建的接口。动态接口有时也被称为用户接口，它使用的 IP 地址属于无线客户端 VLAN 的子网。

通常，预留一个管理 VLAN 和子网供 WLC 和 CAPWAP 使用，可以将管理子网中的 IP 地址分配给管理接口和 AP 管理器接口。所有来自外部的管理数据流（基于 Web，Telnet，SSH 或 AAA）和 CAPWAP 隧道数据流都将到达这些地址，LAP 将被放置到网络的各个地方，甚至是不同的交换模块中，因此应将 LAP 数据流视为外部数据流。

分配给 LAP 的 IP 地址不必属于 AP 管理器子网。在小型网络中，LAP 和 WLC 可能位于同一个子网中，因此它们在第二层是相邻的；在大型网络中，LAP 将分散在不同的交换模块中，LAP 和 WLC 的 IP 地址将各不相同，因为它们不是第二层邻居，这些地址将不属于 AP 管理子网。

图 4-1 说明了一种情景，其中包含各种 WLC 接口以及这些接口的 IP 地址和所属的 VLAN，WLC 的集散系统端口实际上是一条中继链路，它连接 WLC 和 AP 管理子网。此例子对 Cisco WLC 2006，WLCM，440X 和 WiSM 等系列的 WLC 设备都是适用的。

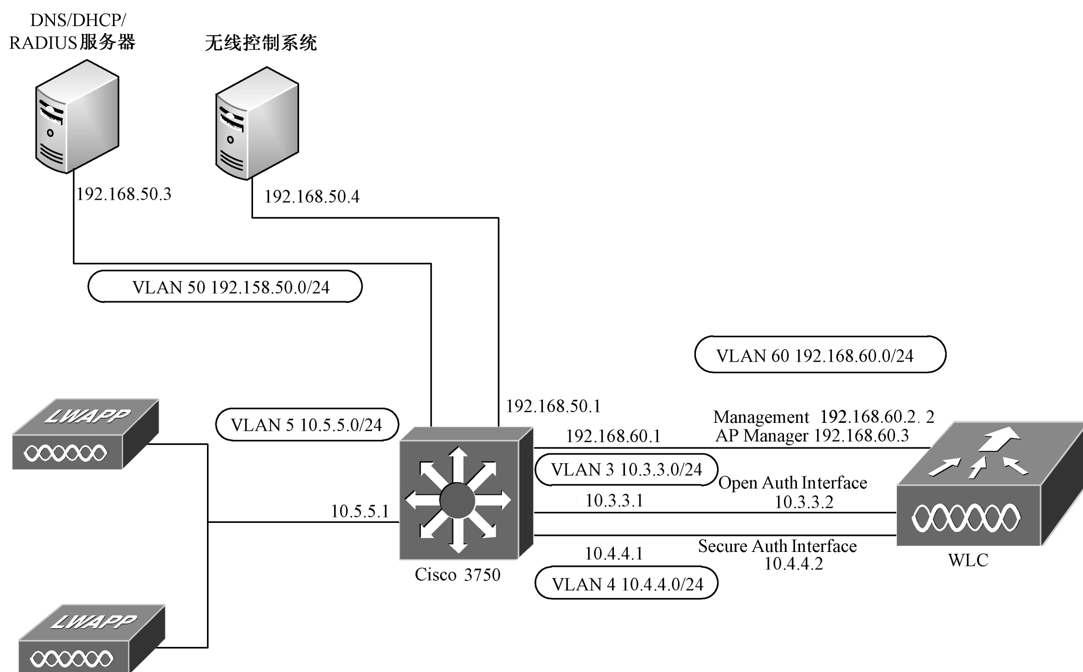


图 4-1　WLC 接口布局示例

在这个例子中，WLC 通过物理端口 1（Port1）连接到 Cisco 3750 交换机的 gig 1/0/1 千兆端口，WLC 上所有的接口（Interface）都映射到物理接口 1。WLC 上配置了两个 WLAN，其中一个是开放认证（使用 Web Portal 认证，SSID 为 Open），另一个是采用 EAP 认证（SSID 为 Secure），分别为开放的 SSID 和 EAP SSID 创建了一个动态接口并同相应的 VLAN 相关联：开放的 SSID 同 VLAN 3 相关联，VLAN 4 同加密的 SSID 相关联。管理端口（Management Interface）和 AP 管理接口（AP Manager Interface）都使用 VLAN 60。为了使配置简单，我们忽略了服务端口（Service-port），所有的网络服务（AAA，DHCP 和 DNS）都使用 VLAN 50，AP 将连接到 VLAN 5。

4.1.2　配置相邻的接入交换机

如图 4-1 所示，WLC 只通过 Port1 连接到 Cisco 3750 接入交换机。Cisco 3750 接入交换机的端口被配置成 IEEE 802.1q 的 Trunk，在此 Trunk 的链路上只允许 VLAN 2～VLAN 4 和 VLAN 60 通过；Management 和 AP-Manager VLAN 采用打标记（Tagged）的 VLAN，而没有被配置成本地 VLAN（Native VLAN），所以在 WLC 上配置这些端口时，必须给它们分配 VLAN 的号码。

IEEE 802.1q 的端口配置如下：

```
interface GigabitEthernet1/0/1
description Trunk Port to Cisco WLC
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2-4,60
switchport mode trunk
no shutdown
```

在配置 Trunk 时，只允许合适的 VLAN 通过，将其他的 VLAN 都修剪掉，这可以减少 WLC 收到的报文数量，提高整个机器的处理性能。

4.1.3　配置 Cisco 无线网络控制器

WLC 的初始化配置只能通过连接到 WLC 控制台端口（Console）的 Cisco 标准 9600-8-N-1 电缆进行，然后使用 Startup Wizard，通过 CLI 输入参数，在 WLC 启动并运行其代码映像，CLI 就将以交互的方式提示输入下面的信息。

① 系统名：一个标识 WLC 的字符串，最多可包含 32 个字符。

② 管理用户名和密码：分别默认为 admin 和 admin。

③ 服务端口的 IP 地址（DHCP 或静态地址）：如果选择使用静态地址，将提示您输入 IP 地址、子网掩码、默认网关和管理接口的 VLAN 号；如果管理 VLAN 没有被标记（中继链路上的本地 VLAN，Native VLAN），请输入 VLAN 号 0。

④ DHCP 服务器的地址：客户端服务器将从 DHCP 服务器那里获得其 IP 地址。

⑤ AP 管理器接口的 IP 地址。

⑥ 虚拟接口的 IP 地址：一个伪造的 IP 地址，通常为 1.1.1.1。

⑦ 移动组名称：在属于同一个移动组的所有 WLC 上都必须相同。

⑧ 默认的 SSID：LAP 加入控制器时将使用它，当 LAP 加入后，WLC 将把其他 SSID 提供给它。

⑨ 是否要求客户端从 DHCP 服务器那里获得 IP 地址？如果要求客户端使用 DHCP 服务器，则输入 yes，否则输入 no；允许客户端使用静态配置的地址。

⑩ 是否需要配置 RADIUS 服务器？可以输入 NO，通过 Web 前端配置 RADIUS 服务器。

⑪ 配置国别码：输入 help 可获悉国别码列表，中国的国别码为 CN。

⑫ 在 WLC 管理的所有 AP 上启用 / 禁用 IEEE 802.11b 和 IEEE 802.11g：在系统提示您配置每种 WLAN 时，输入 YES 可启用它，输入 NO 将禁用它。

⑬ 启用 / 禁用射频源管理 auto-RF 功能：输入 yes 将启用 RF 参数自动调整，输入 NO 将禁用它。

在输入上述信息后，WLC 将存储配置并重新启动，然后，便可以通过 WLC 的 Web 界面管理它。

以下是配置的详细步骤（大写选项为默认值）：

```
（Cisco Controller）
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...

System Name [Cisco_ f1:11:04]（31 characters max）:
AUTO-INSTALL: no interfaces registered.
AUTO-INSTALL: process terminated -- no configuration loaded
Enter Administrative User Name（24 characters max）: admin
Enter Administrative Password（24 characters max）: *******
Re-enter Administrative Password                   : *******
Service Interface IP Address Configuration [none][DHCP]:
Enable Link Aggregation（LAG） [yes][NO]:
Management Interface IP Address: 192.168.60.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.60.1
```

```
Management Interface VLAN Identifier（0 = untagged）: 60
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 192.168.50.3
Enable HA [yes][NO]:
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: CISCO

Network Name（SSID）: secure
Configure DHCP Bridging Mode [yes][NO]:
Allow Static IP Addresses [YES][no]:
Configure a RADIUS Server now? [YES][no]:
Enter the RADIUS Server's Address: 192.168.50.3
Enter the RADIUS Server's Port [1812]:
Enter the RADIUS Server's Secret: star
Enter Country Code list（enter 'help' for a list of countries） [US]: CN
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:
Configure a NTP server now? [YES][no]:
Enter the NTP server's IP address:192.168.50.5
Enter a polling interval between 3600 and 604800 secs: 3600
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

当重启完成后，就可以使用 Web 方式配置 WLC。打开浏览器，在地址栏中输入 https://192.168.60.2，输入正确的用户名与密码后，得到如图 4-2 所示的欢迎页面。

若要更改系统名称，单击 CONTROLLER 选项卡，在 Name 栏目中输入合适的系统名称并应用，系统的名称就会即时更改，如图 4-3 所示。

4.1.4　进一步配置 WLC

WLC 使用动态接口将集散在系统端口上的 VLAN 扩展到无线局域网，可以采取下面的步骤来配置 WLC 所在的 WLAN：

① 创建一个用于无线客户端的动态接口；

② 创建一个绑定到动态接口的 WLAN。

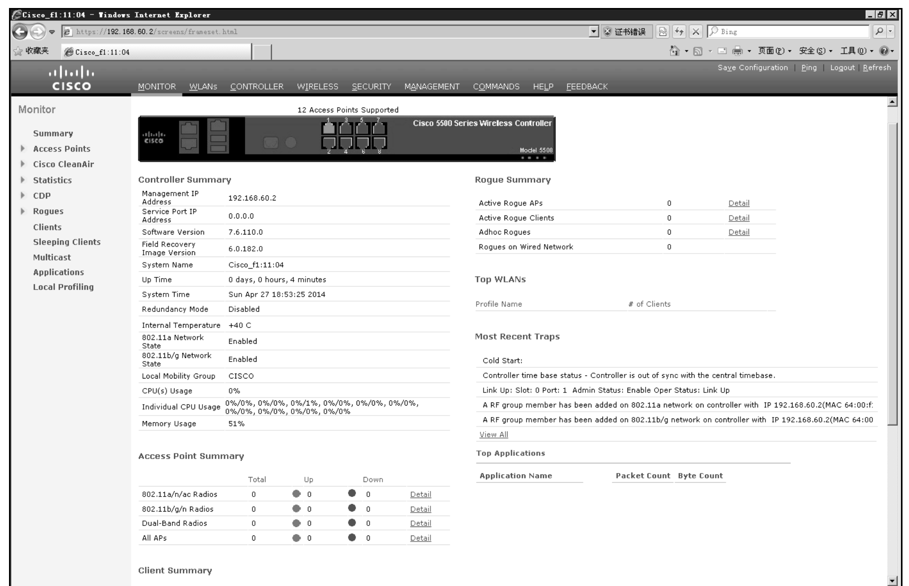


图 4-2 WLC Web 管理导航页面

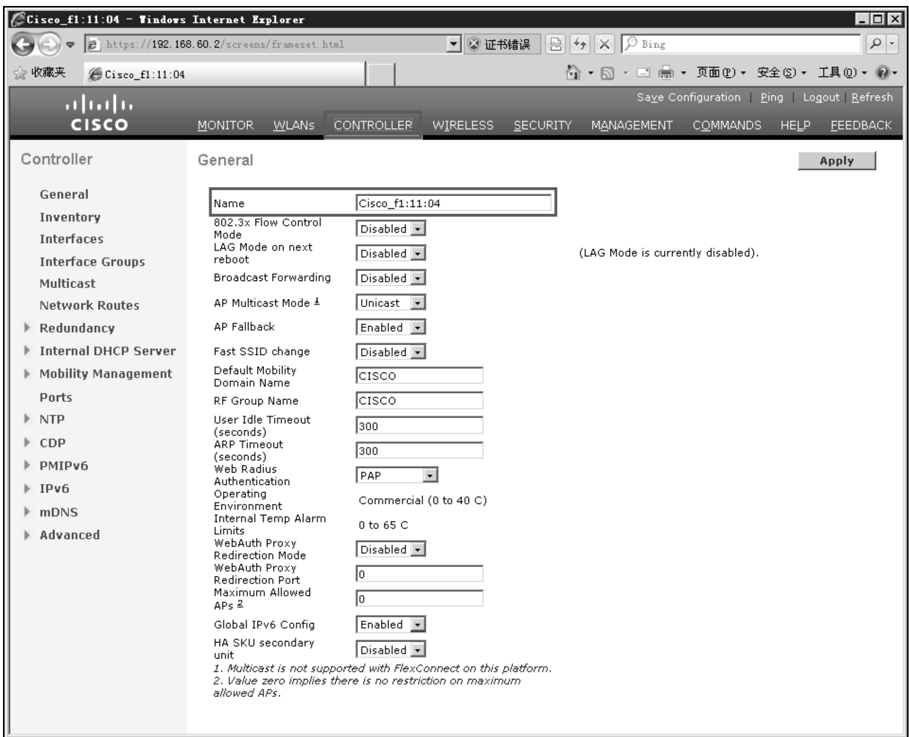


图 4-3 更改系统名称

就图 4-1 所示的接口位置和地址分配情况而言，应首先为客户端 VLAN3 和 VLAN4 创建动态接口。为此，可单击 WLC 任务栏中的 CONTROLLER 选项卡，然后单击左边的 Interfaces，再单击 New 按钮切换到如图 4-4 所示的屏幕。在这里，可以给动态接口指定一个描述性名称（Open-Auth-Vlan-3），并将其绑定到特定的 VLAN ID 3（如图 4-5 所示），设置完成后，单击 Apply 按钮。

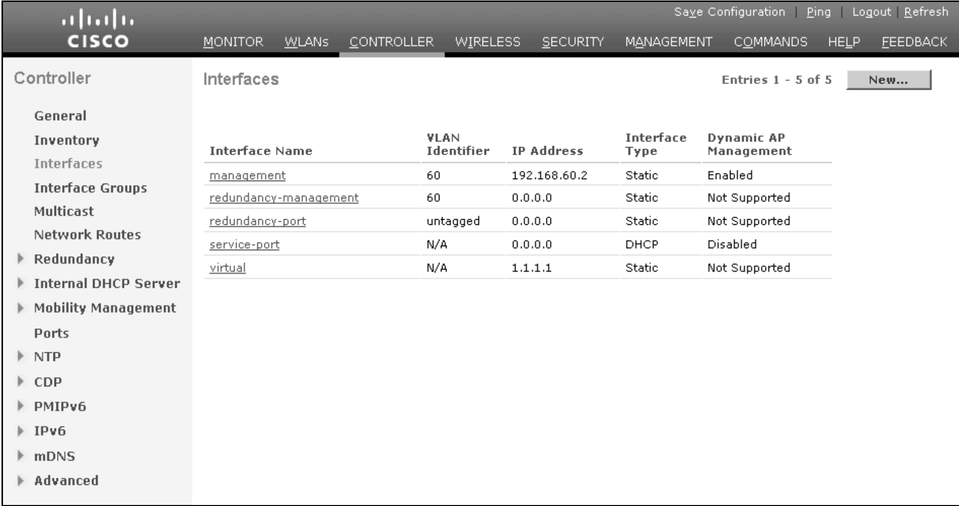


图 4-4　创建用户端动态端口

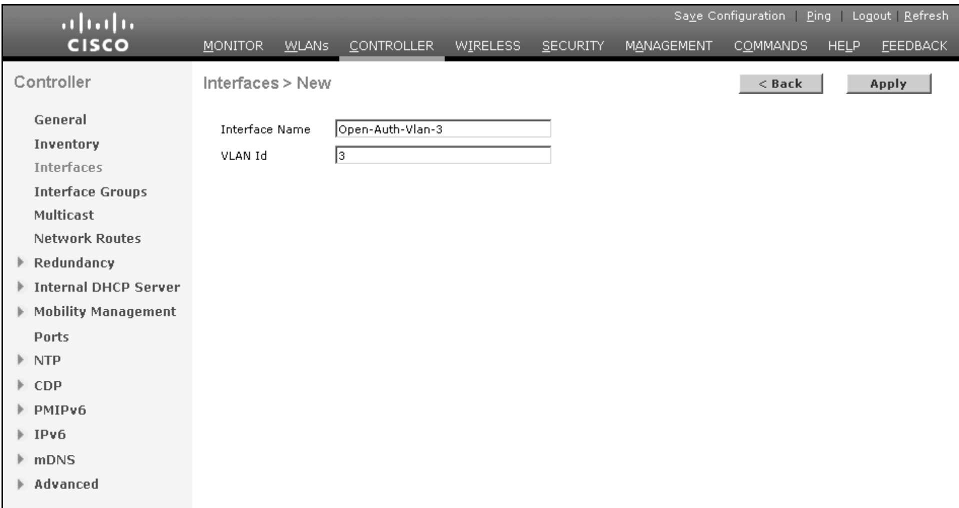


图 4-5　在 WLC 上创建动态接口 Open-Auth-Vlan-3

接下来，必须给新的动态接口提供编址信息，WLC 显示如图 4-6 所示的屏幕，WLC 还必须有用于无线客户端子网的 DHCP 服务器的地址，因为它为广播 DHCP 请求的客户端充当 DHCP 中继。

图 4-6　给 Open-Auth-Vlan-3 动态接口设置编制信息

重复上述步骤，为 VLAN4 创建动态接口，如图 4-7 和图 4-8 所示。

接下来，需要定义一个 WLAN，它将为无线客户端提供服务，且与加入到该 WLC 的 LAP 相关联。单击 WLC 任务栏中的 WLANs 选项，在下拉框中选择 Create New，然后单击 Go 按钮。在如图 4-9 所示的 WLANs>New 屏幕中，输入 WLAN 将使用的 SSID（这里为 open），输入 Profile Name（open-auth，是一个配置文件）。



图 4-7　在 WLC 上创建动态接口 Secure-Auth-Vlan-4

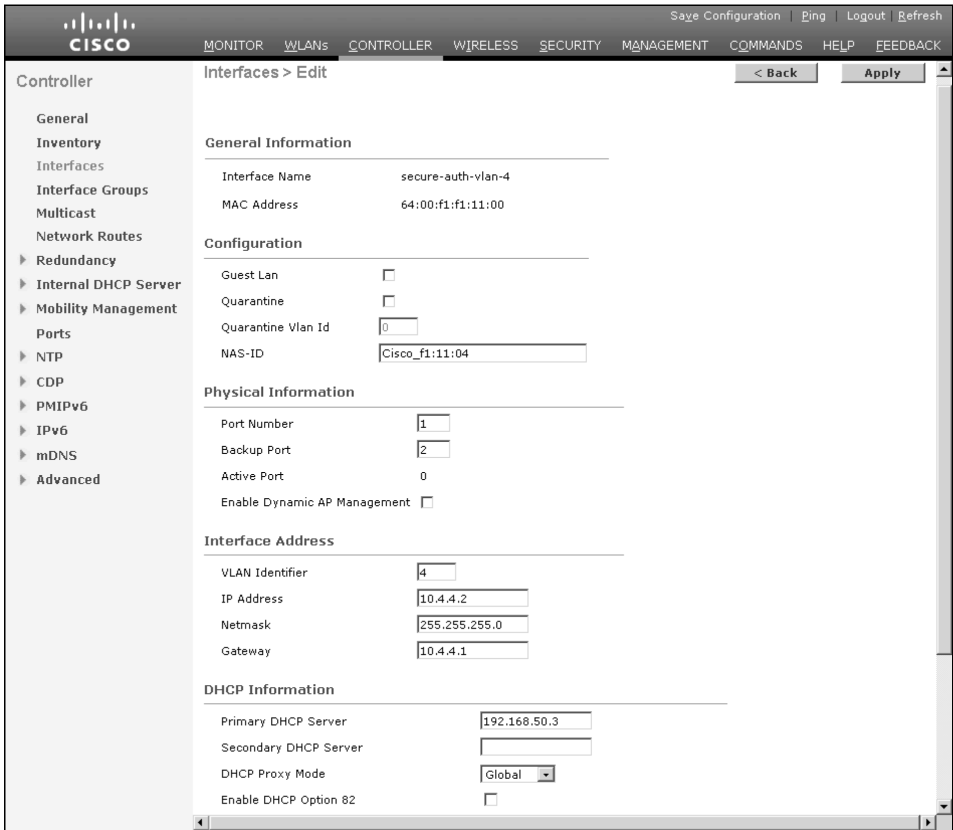


图 4-8　给 Secure-Auth-Vlan-4 动态接口设置编制信息

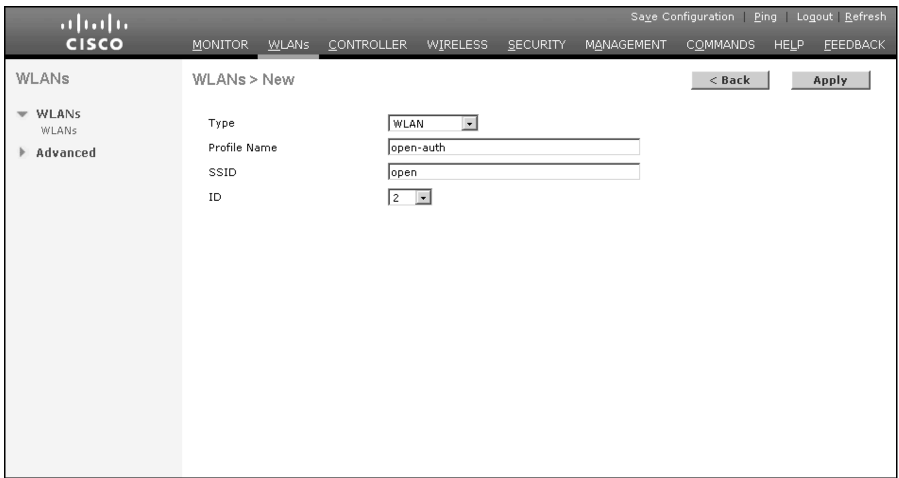


图 4-9　定义一个新的 WLAN

单击 Apply 应用后，WLC 将显示如图 4-10 所示的 WLANs>Edit 屏幕。在这里，需要将 SSID 同一个动态接口关联起来。从下拉列表 Interface 中选择前面创建的动态接口。在这个例子中，将 SSID open 绑定到动态接口 open-auth-vlan-3。

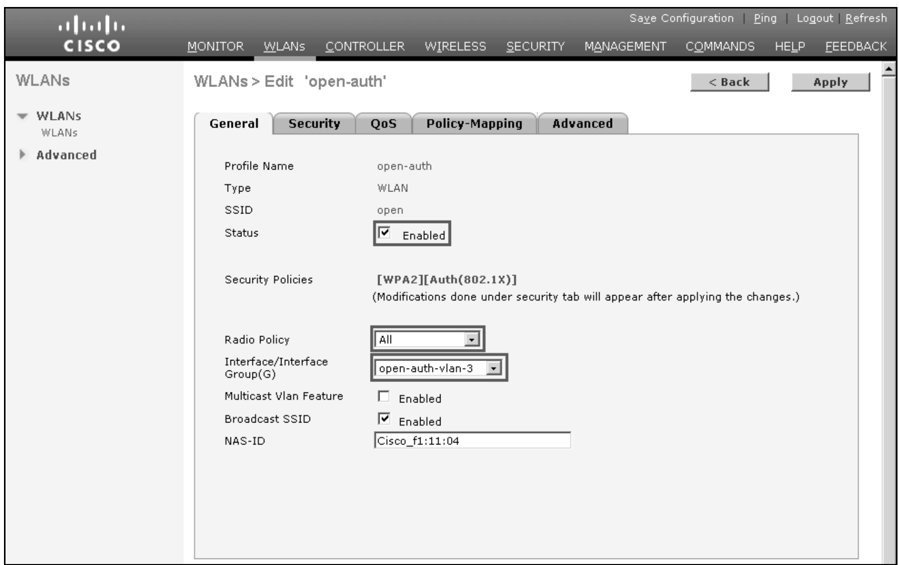


图 4-10　将 WLAN 绑定到动态接口

注意

将 Status 的复选框改为 Enabled，以使能此 WLAN；在 Radio Policy 下拉列表中可以选择无线频谱，如果要使能 IEEE 802.111a/b/g，则选择 All。

由于此 WLAN 是开放模式，我们需要将 WLANs>Edit>Security>Layer 2 中的 Layer 2 Security 改为 None，禁用第二层的安全性，如图 4-11 所示。



图 4-11　禁用第二层的安全性

在 WLANs>Edit>Security>Layer 3 中，将 Layer 3 Security 选为 Web Policy，选择 Authentication，采取 Web Portal 的方式认证用户，即当用户访问网络时，IE 会自动弹出认证页面让用户输入用户名与密码进行认证，如图 4-12 所示。



图 4-12　开启第三层 Web Portal 认证

最后，需要为认证指定认证服务器，在 WLANs>Edit>Security>AAA Servers 中，在 Radius Servers 选择认证服务器，如图 4-13 所示。

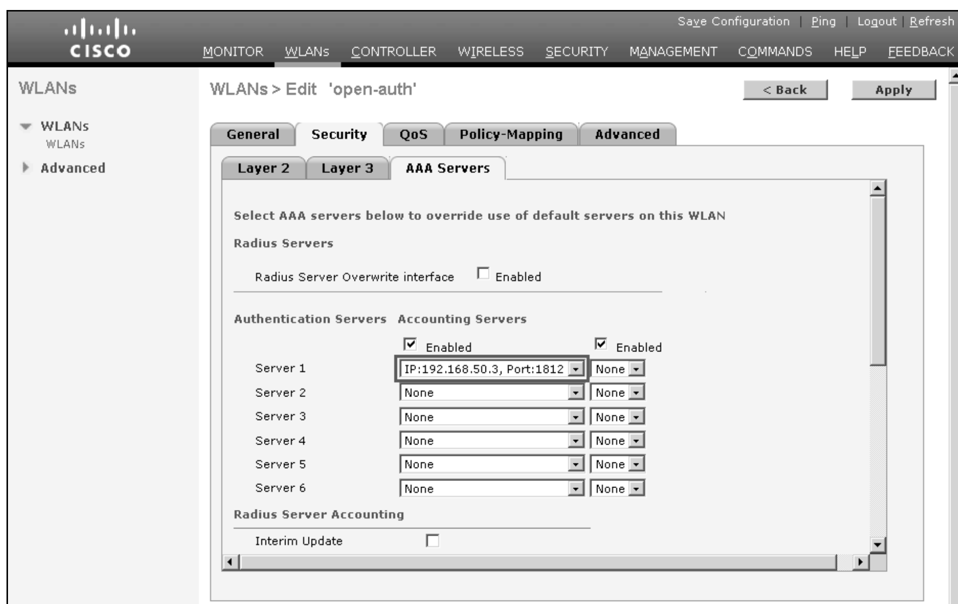


图 4-13　认证服务器设置

为 secure 的 SSID 建立 WLAN，在 WLANs 标签下单击 secure 的 WLAN ID，如图 4-14 所示。

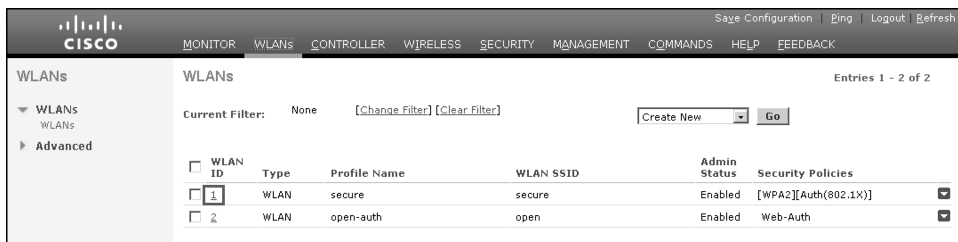


图 4-14　设置 Secure 的无线配置文件

在 General 选项标签中，将 Interface 选项从默认的 management 改为前面创建的 secure-auth-vlan-4，如图 4-15 所示。

接下来设置第二层的认证方式，在 Security 选项卡中选择 Layer 2 选项卡，设置安全方式为 IEEE 802.1X，当用户接入时采用 IEEE 802.1X 认证。详细配置方式如图 4-16 所示。

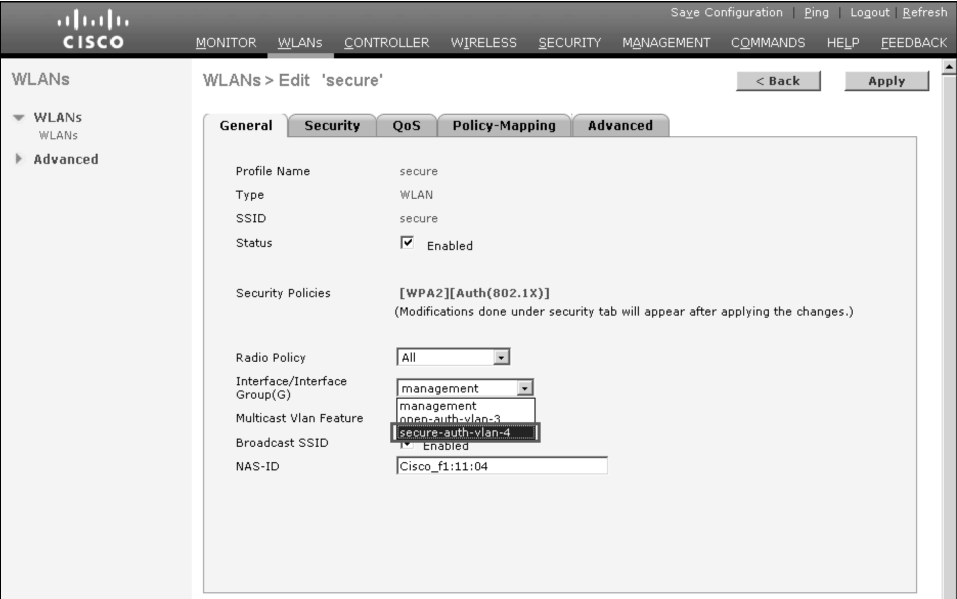


图 4-15　更改 Secure 的 Interface

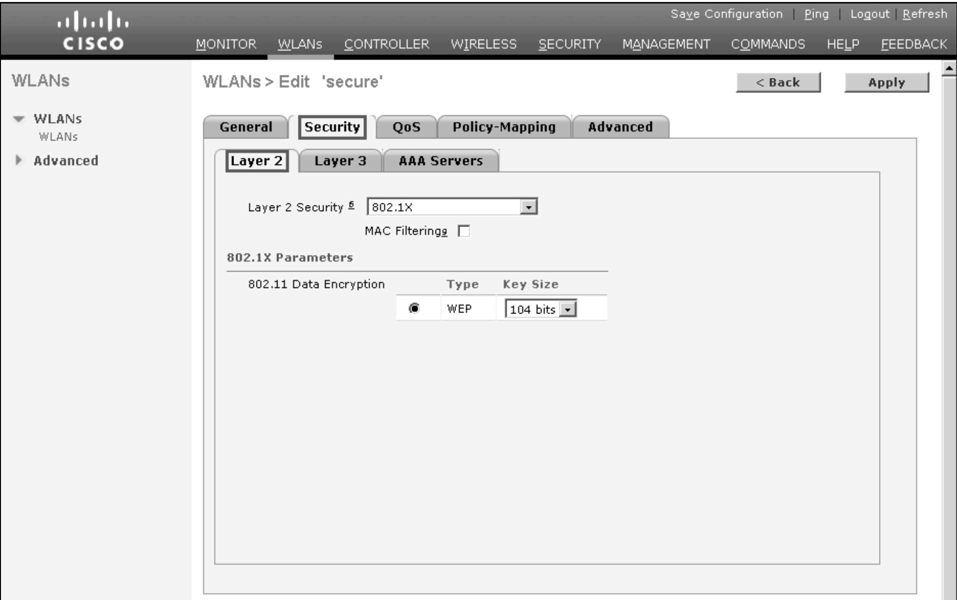


图 4-16　第二层认证方式的选择

关于第二层认证方式，有多种选择，各种认证方式的描述如表 4-1 所示。

表 4-1 第二层认证方式总结

参　　数		描　　述
Layer 2 Security	None	没有选择任何第二层安全性
	WPA+WPA2	采用 WiFi 保护的方式接入
	IEEE 802.1X	采用 IEEE 802.1X 的方式接入
	Static WEP	采用 WEBP 加密的方式接入
	Static WEP + IEEE 802.1X	既采用 WEBP 方式接入，同时又采用 IEEE 802.1X 的认证方式
	CKIP	采用 Cisco Key Integrity Protocol （CKIP）加密方式
MAC Filtering		采用 MAC 地址过滤，只有列表中的 MAC 地址才能通过认证

4.1.5 配置 AP 组

在默认部署情况下，一个 WLAN 只能被映射到 WLC 上的一个端口（即一个 VLAN）。设想一种情况，当采用 5508-100 类型的 WLC 时，共可以承受 100 个 AP 的接入，以每个 AP 平均接入 25 个用户计，共可能接入 2 500 个用户，这样就需要 2 500 个 IP 地址，如果只采用一个 VLAN，就需要 16 个 C 类 IP 地址（255.255.240.0 或/20）的网段供使用，这将产生很大的广播风暴不说，还会造成极大的 IP 地址浪费。

为了克服以上的情况，需要创建多个比较小的用户域，这就需要用到 AP Group 的特性，同时还需创建基于地域的 VLAN，值得注意的是，AP Group 不支持组播。

在图 4-17 中，共配置了 3 个动态端口，分别映射到 3 个基于地域的 VLAN——VLAN61，VLAN62 和 VLAN63。这些基于地域的 VLAN 将应用到 secure 的 SSID，当用户关联到那些绑定到 VLAN61 的 AP 上时，将会取到属于 VLAN61 地址池的 IP 地址，关联到属于 VLAN62 的 AP 用户将会得到 VLAN62 地址池的 IP 地址，在不同的基于地域的 VLAN 之间漫游时，将会被控制器当作控制器内部的三层漫游，用户可以保持他们原先的 IP 地址。

配置支持基于地域 VLAN 的 AP Goup 需要以下三个步骤：

① 配置好相应的动态接口，并把它们映射到所希望的 VLAN 中；

② 创建好 AP Group；

③ 将 AP 分配到相应的 Group 中。

如果需要配置图 4-17 中的 AP Group，需要为 VLAN61，VLAN62 和 VLAN63 分别创建动态端口。参考图 4-18 创建 AP Group，转到 WLANs>Advanced>AP Groups，点击 Add Group 按钮。

为 Group 设置名称和描述后单击 Add 按钮。

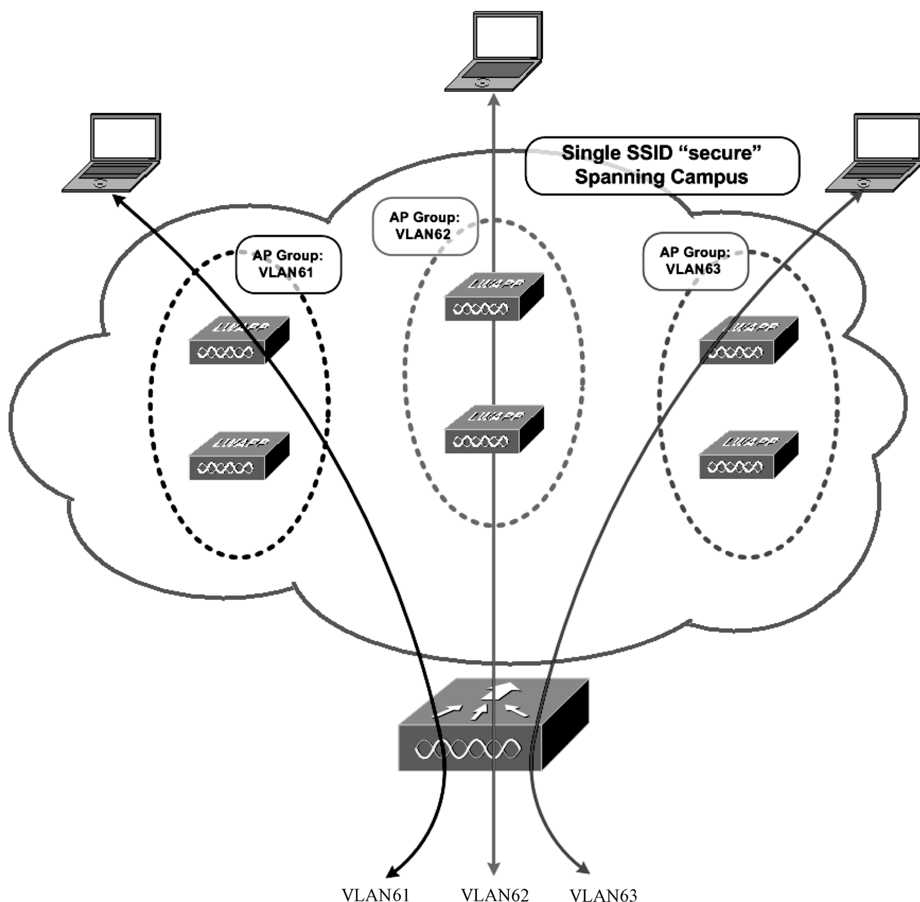


图 4-17　AP Group 以及基于地域的 VLAN

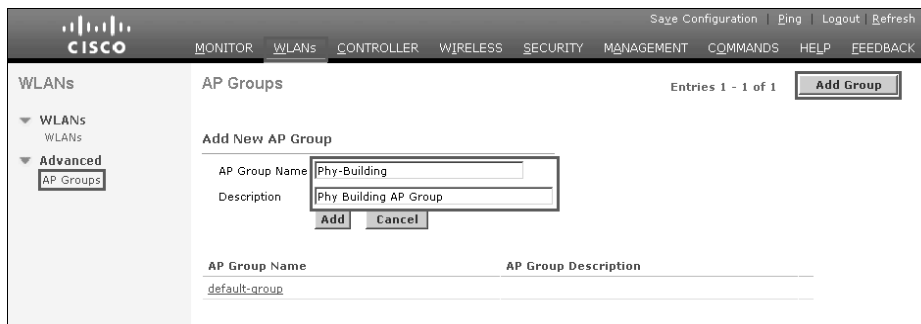


图 4-18　创建 AP 逻辑分组

打开刚创建的 AP Group，在 WLANs 选项卡下单击 Add New，选择一个 WLAN 的 SSID 及一个合适的端口名称（如图 4-19 所示），然后单击 Add 按钮。注意：如果我们的系统同时存

在多个 WLAN 配置文件，则需要为每个 WLAN 都创建 AP Group 的映射，换句话说，每个 WLAN 都必须包括在 AP Group 中，但并不需要每个 Interface 都是基于地域的。比如，我们建立了一个 Guest 的 SSID 后，希望在全校的无线 AP 上都广播这个 SSID，但是 Guest 的用户不是很多，一般为 100 个左右，我们就可以只为 Guest 创建一个 Interface，并将它映射到只包含/25 的 VLAN 中在 AP Group 中，将所有的 Group 都映射到同一个 Interface 上。

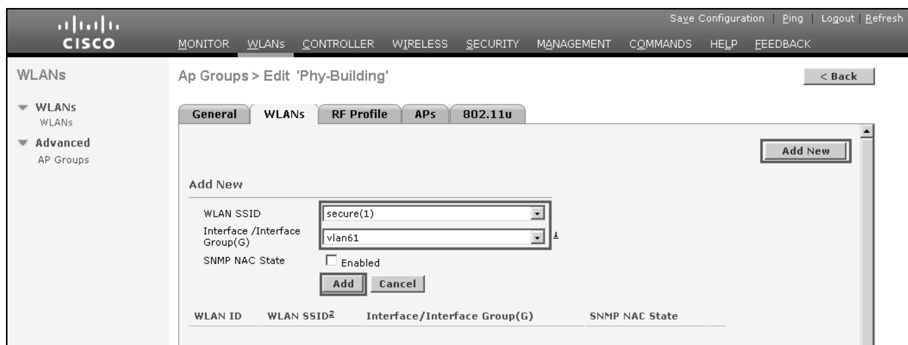


图 4-19 将 AP 分组映射到动态端口上

重复以上的步骤，为每个 AP Group 建立映射关系。

下面就需要将 AP 加入对应的 AP Group。

转到 Wireless>Access Points>All APs，点击 AP 名字，打开 AP 的状态，选择其中的 Advanced 标签，从 AP Group 中选择合适的 Group 并单击 Apply，如图 4-20 所示。

如果 WLC 运行的是 6.0 及以上高版本的映像软件，则在 WLANs>Advanced>AP Groups 中选择相应的 AP Group 并打开后，选择 APs 标签，从右侧选择合适的 AP 加入到 AP Group 中。注意：将 AP 加入到 AP Group 中将会引发 AP 的自动重启，这对用户的网络访问可能会造成一定的影响，如图 4-21 所示。

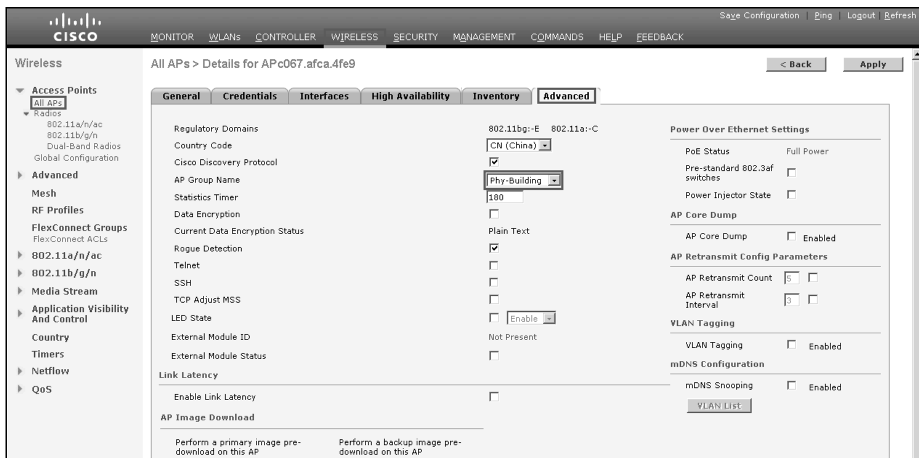


图 4-20 将指定 AP 划入相应的 AP 分组

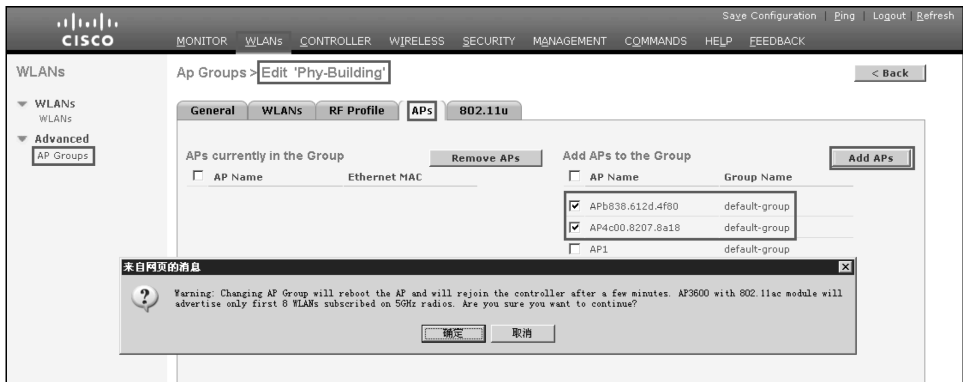


图 4-21　高版本 WLC 中将 AP 批量加入 AP 分组

4.1.6　配置移动组

前面讲过，为使用户漫游到与不同的 WLC 关联的 LAP 中而仍然保持网络的畅通，这些 WLC 必须同属于一个移动组（Mobility Domain Group）。

在配置移动组之前，必须确保所有 WLC 管理的 IP 地址第三层可通。移动组是在初始化 WLC 时配置的，我们也可以在初始化完成后通过 GUI 的界面修改移动组的名称，具体位置在 Controller > General 页面中的 Default Mobility Domain Name，移动组的名称区分大小写。

对于 Cisco 的 WiSM，由于其中内置了两个 4400 控制器，这两个控制器必须属于同一个移动组，以便支持 300 个 AP 的无缝漫游。移动组中所有的 WLC 必须配置相同的虚拟 IP 地址。管理员必须手工获取所有 WLC 的 MAC 地址和 IP 地址。

导航到 Controller > Mobility Management > Mobility Groups，打开 Static Mobility Group Members 页面，如图 4-22 所示。此页面显示了默认的移动组名称，同时列出了所有控制器的 MAC 地址及 IP 地址，列表中的第一条记录是本地控制器的信息。

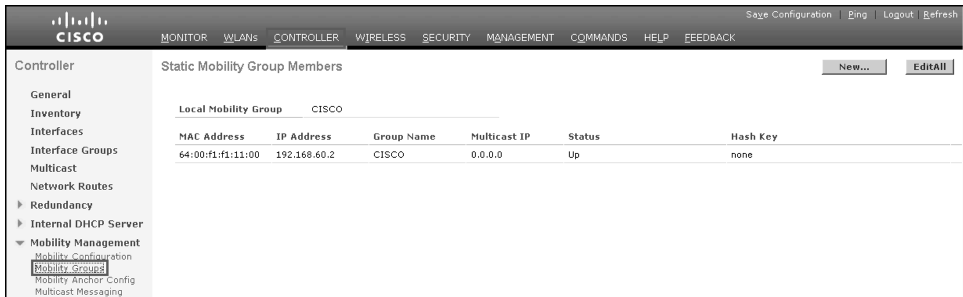


图 4-22　配置静态移动组成员

单击 New 按钮增加组中其他 WLC 的 MAC 地址及 IP 地址，如图 4-23 所示。

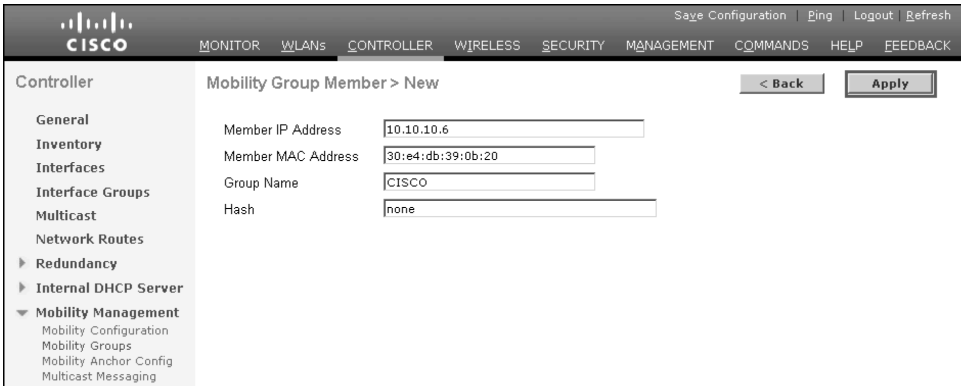


图 4-23　增加移动组中 WLC 的 MAC 及 IP 信息

增加完成后，单击 Apply 按钮和 Save Configuration 应用以保存配置。如果需要，可以单击图 4-22 中的 Edit All 按钮，将会在列表框中显示本移动组中所有的控制器信息，管理员可以任意编辑及删除相关控制器的条目，如图 4-24 所示。



图 4-24　编辑本移动组中所有控制器的信息

选择 Multicast Messaging，打开 Mobility Multicast Messaging 页面，选中 Enable Multicast Messaging 的复选框，输入本地移动组播地址，控制器将会使用组播模式发送 Mobile Announce Messages 给组中的成员，如图 4-25 所示；否则还是通过单播传送相关的宣告报文。

为了配置 3.2.4 节中的静态 IP 地址漫游，导航到 WLANs>选择某个 WLAN>Advanced，选中 Static IP Tunneling 边上的复选框，以允许静态 IP 地址漫游，如图 4-26 所示。如果采用 CLI 方式配置，则在 CLI 模式下输入：



图 4-25　配置本地移动组组播地址

```
(WLC) >config wlan static-ip tunneling {enable | disable} <wlan-id>
enable          在特定的 WLAN 上使能 static IP tunneling 支持
disable         在特定的 WLAN 上禁止 static IP tunneling 支持
```

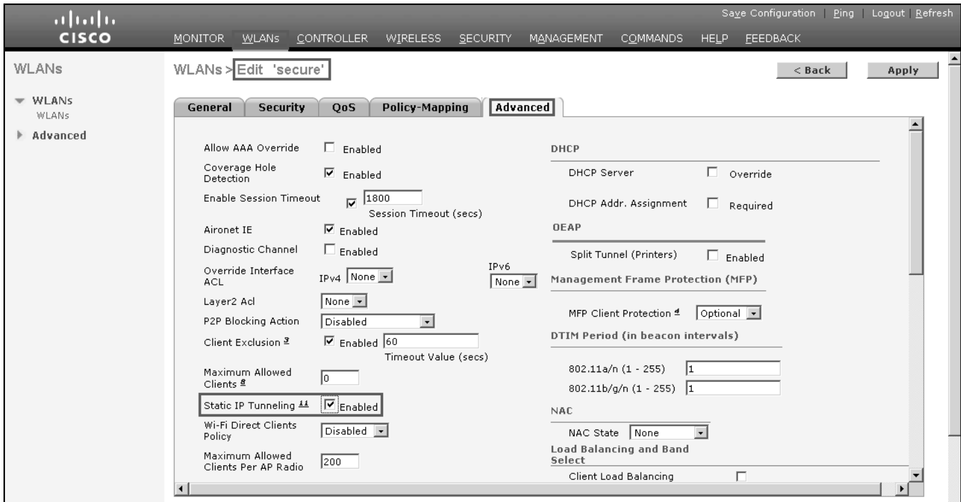


图 4-26　配置静态 IP 地址漫游

4.2　配置 HREAP

HREAP（Hybrid Remote Edge Access Point）是为企业的分支机构及远程办公室 AP 部署的一种设计方案。它让客户在公司办公室可以通过广域网（WAN）配置并控制分支或远程办公

室的 AP 访问点，而无须在每个办公分部都部署无线网络控制器。当 HREAP 与远程总部的控制器失去连接时，可以在本地认证用户并将用户的流量直接发送到本地网络；当 HREAP 重新取得同控制器的关联后，可以再次通过隧道将数据发送回控制器处理。

HREAP 仅支持 1040、1130、1140、1240、1250、3500、1260 和 AP801 无线接入点，只有在 2100、4400 和 5500 系列控制器，Catalyst 3750G 集成控制器，WiSM 和 WiSM2，以及路由器集成控制器上才具有这些功能。

4.2.1 CAPWAP 下 HREAP 的操作

CAPWAP 支持如下两种 AP 的操作。

（1）Split-MAC

在这种模式下，控制器除了处理 IEEE 802.11 的认证及关联信息外，它同时作为用户数据进出的节点，Split-MAC 的隧道将所有的用户数据通过 CAPWAP 的数据通道传输给控制器，反之亦然。

（2）Local-MAC

在本地 MAC 模式下，在 AP 上将实现所有 IEEE 802.11 功能，这样当到控制器的控制连接中断后，远程 AP 可以继续保留无线功能，并将用户的数据通过以太口直接发送到本地网络。这种方式对一些远程分支机构很有用，本地没有无线网络控制器，但仍有部分 AP 需要通过广域网连接到总部。

在 4.0 或更高版本的无线控制器上，可以在 AP 上同时实现以上两种功能，即远端无线客户端的数据既可以在本地直接分发，也可以通过隧道传回到控制器并通过控制器端的路由分发，如图 4-27 所示。

4.2.2 HREAP 的核心概念

为了实现本地及集中的数据分发，HREAP 有如下两种不同的模型。

① 集中及本地分发：在 HREAP 上的 WLAN 可以配置成将用户的流量全部通过中心的控制器集中分发或直接将流量通过本地有线以太网口直接进入本地交换网，本地交换的 WLAN 数据在通过以太网络时通常带有 IEEE 802.1q 的标签。

② 连接及独立状态：当能够同控制器取得联系时，HREAP 工作在连接状态，一旦同控制器失去联系，HREAP 将工作在独立状态。然而无论处于连接状态还是独立状态，有关用户的验证等全局安全操作都需要控制器参与，一旦失去同控制器的联系，远程 AP 将不能响应这些事件。

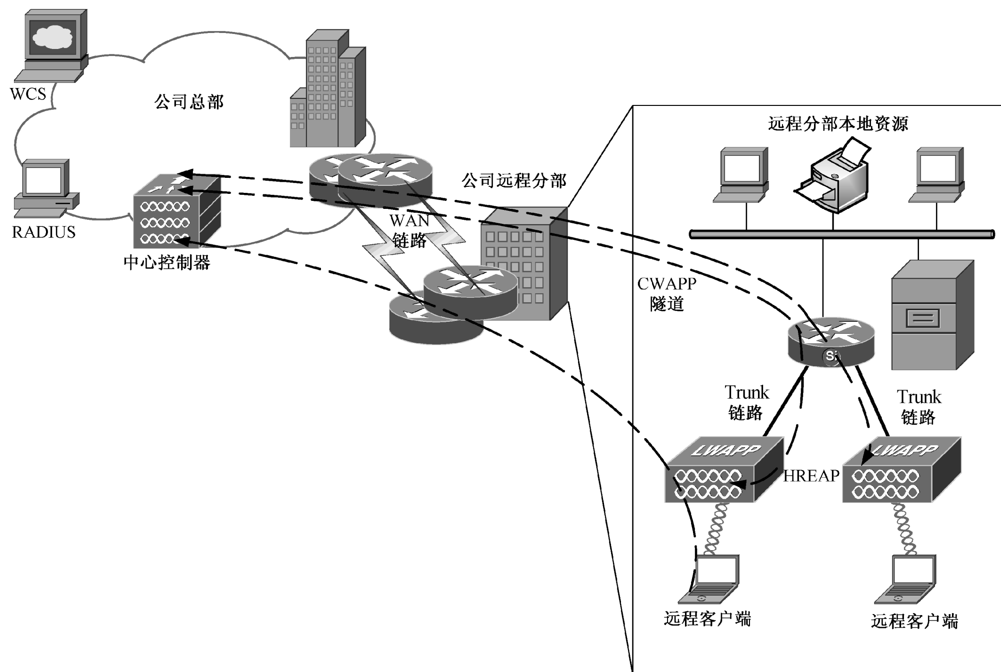


图 4-27　HREAP 远程连接示意图

当一个用户同 HREAP 上的某个 SSID 关联后，AP 将用户所有的认证报文发到控制器进行认证，一旦成功进行认证，根据 SSID 所对应的 WLAN 的配置，用户的数据就可以通过隧道传到控制器进行处理或在本地直接转发。根据用户验证机制及数据转发操作，HREAP 上的 WLAN 可以配置成如下几种状态。

① 中心认证，中心转发：在这种状态下，对于给定的 WLAN，AP 将所有的用户认证请求及用户数据发回到控制器进行处理，当然这种状态仅当 AP 到控制器的 CWAPP 隧道处于连接状态时存在。

② 中心认证，本地转发：在这种状态下，对于给定的 WLAN，控制器处理所有的用户认证，而 HREAP 将在本地转发所有的用户数据，当用户成功认证后，控制器通过 CWAPP 的控制隧道指示 HREAP 在本地转发所有的用户数据。

③ 本地认证，本地转发：在这种状态下，HREAP 在本地对用户进行认证，在本地直接转发用户的数据。此时 WLAN 只能配置成二层开放、共享的认证方式，如 WPA-PSK 和 WPA2-PSK，其他诸如用户名和密码等认证方式只能在连接状态下由控制器完成。

④ 认证关闭，本地转发：这种状态只能工作在独立状态下，对于给定的 WLAN，HREAP 拒绝所有的新用户认证，而仍然保持同已经接入并成功认证用户的连接状态。当配置了 EAP、动态 WEP、WPA、WPA2、IEEE 802.11i、Web Portal 和 NAC 等需要控制器参与的认证方式时，若 CWAPP 控制链路失败，HREAP 就从“中心认证，本地转发”状态进入“认证关闭，本地

转发”状态。一旦用户的密钥或会话超时，用户将无法再次接入网络。当 HREAP 上的某个 WLAN 没有与之关联的用户时，将不会再发送某个 SSID 的信标报文，HREAP 将进入下一个要讲述的状态——“认证关闭，转发关闭”状态。（注意，在 5.2 及更高版本中，允许在 HREAP 本地配置 RADIUS 服务。）

⑤ 认证关闭、转发关闭：这种状态只在独立模式下才会出现，此时 HREAP 已经关闭了所有的用户连接，不再广播 SSID 的信标报文。

4.2.3 HREAP 的配置

因为 HREAP 是用来在跨越广域网的链路上实施的，但在配置 HREAP 功能时，需要注意如下几点。

- HREAP 的 AP 可以被配置成静态或动态的 IP 地址，如果设置动态的 IP 地址，则在 AP 启动时，应该能够从本地的 DHCP 服务器顺利取得一个 IP 地址。
- HREAP 支持仅有 500 字节的广域网分片。
- 在跨越广域网链路时，应该首先保证 CAPWAP 控制报文的优先级，链路的数据传输 RTT 应该控制在 300 ms 以内，语音传输应该控制在 100 ms 以内。
- 当采用 HREAP 方式时，组播流量只能通过单播来实现。
- 为了在 HREAP 的 AP 之间实现 CCKM 快速漫游，应该在控制器上配置 HREAP 的组。
- HREAP 支持在单个 AP 上广播多个 SSID。
- 为了更方便管理 HREAP 的接入点，需要定义一个 HREAP 的 AP 组，在这个组中的 AP 共享 CCKM、WLAN 以及备份 RADIUS 的配置，每个控制其上可以配置 20 个 AP 组，每个组最多可包含 25 个 AP。

在 5.0.148 及更高版本的映像软件中，HREAP 组支持如下两个新特性。

- 备份 RADIUS 服务器：可以在控制器上配置处于独立状态的 HREAP 的 AP 使用备份 RADIUS 服务器进行 IEEE 802.1X 认证。当然，除了配置备份 RADIUS 服务器外，还可以配置 Primary 和 Secondary 的 RADIUS 服务器。
- 本地认证：可以通过控制器配置 HREAP 在本地进行认证，早期版本最多可在 AP 上配置 20 个静态用户，5.0 以后的版本支持 100 个静态用户。当 AP 在控制器上注册时，控制器将会下发用户列表给所有的 HREAP。

当将 HREAP 的有线以太口配置成 TRUNK 模式时，AP 将 CAPWAP 的报文通过 Native VLAN 传输，本地转发的数据可以通过 Native VLAN 或其他有标记的 VLAN 传输。当 HREAP 上存在多个需要本地转发的 WLAN 时，最好配置 Trunk 模式。

HREAP 不支持以下几个功能。

- 当 HREAP 处于“中心认证，本地转发”模式时，不支持控制器的外部 Web 认证，但内部 Web 认证仍然支持。

- 当配置了本地转发的 WLAN 时，不再支持第三层的漫游，如果需要第二层的漫游支持，则需要在所有的 HREAP 上配置一个公共的 VLAN 地址段。
- HREAP 不再支持控制器端的 NAT 及 PAT 地址转换。
- 本地转发的 WLAN 不再支持控制器端的 ACL，中心转发的 WLAN 仍然支持。
- HREAP 不再支持 WGB。

配置 HREAP 时首先要配置 AP 的本地接入交换机，配置流程如下：

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99
ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

在此例程中，HREAP 同交换机的第一端口相连，并通过 Native VLAN10 从交换机获得一个 IP 地址，VLAN11～VLAN12 用来指派给与之相连的 WLAN。

与之相关的路由器配置如下：

```
ip cef
frame−relay switching
class−map match−all 1
match access−group 199
policy−map mypolicy
class 1
bandwidth 256
!
interface Serial0/0
ip address 10.1.0.2 255.255.255.0
encapsulation frame−relay
frame−relay interface−dlci 101
frame−relay intf−type dce
service−policy output mypolicy
! 在路由器上指定 CAPWAP 的控制信道的优先级。
access list 199 permit udp any any eq 5246
```

配置一个如表 4-2 所示的 HREAP，其步骤如下所述。

表 4-2　配置 HREAP

WLAN SSID	Security	Switching
Corporate	WPA2(802.1X)	Local
RemoteSite	WPA2-PSK	Local
Guest	WEB Auth	Central

① 导航到控制器的首页，选择 WLANs，在下拉框选择 Create New，单击 Go 按钮（如图 4-28 所示）。

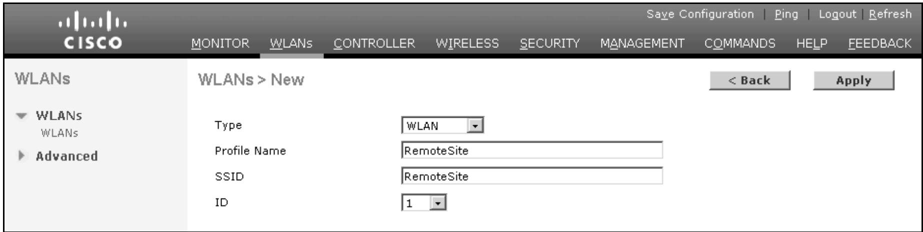


图 4-28　配置 HREAP 的 WLAN

② 指定 WLAN 的名称并单击 Apply 按钮。

③ 在 WLANs>Edit 页面，单击 Security 标签，在 Layer 2 安全标签下，选择安全类别。为了配置 WPA2-PSK，应该选择 WPA+WPA2，如图 4-29 所示。

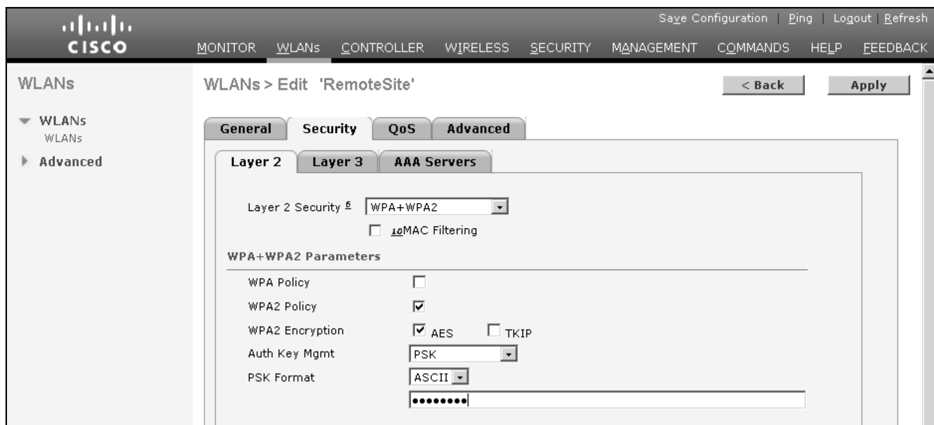


图 4-29　配置 WPA2-PSK

④ 选中 WPA2 Policy 的复选框以便指定 WPA 的相关操作。

⑤ 选择 AES 来设定加密的类别。在 Auth Key Mgmt 下拉框中选择 PSK。为了简便操作，选择 ASCII 格式，并输入预置密钥。

⑥ 选择 Advanced 标签，选中 H-REAP Local Switching，如图 4-30 所示。

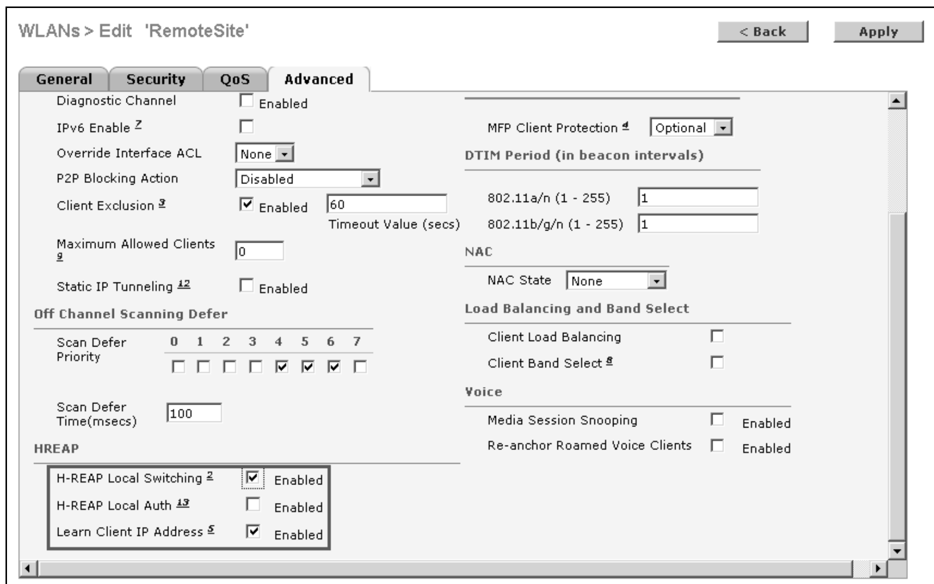


图 4-30　配置 HREAP 本地转发

⑦ 当 AP 发现并加入 WLC 后，导航到 Wireless 并选择相应的 AP，将 AP Mode 改为 H-REAP 模式，并单击 Apply 按钮，AP 将会完成重启并生效，如图 4-31 所示。

图 4-31 配置 AP 的模式为 HREAP

默认情况下，HREAP 不支持 Trunk 方式，为了支持 Trunk 方式的传输，必须在控制器端完成对 AP 的配置。

⑧ 打开 AP 的详细信息界面，选择 HREAP 标签，选中 VLAN Support 的复选框，将 AP 所连接的交换机端口上配置的 Native VLAN 的号码输入框内，本例中为 10，单击 Apply 按钮，如图 4-32 所示。

图 4-32 配置 HREAP Trunk 端口的 Native VLAN ID

⑨ 再次进入此 AP 的详细信息，选择 HREAP 的标签，选择 VLAN Mappings，为每个 WLAN

配置同本地交换机相匹配的 VLAN（当 AP 执行本地转发时客户端获取 IP 地址的 VLAN），如图 4-33 所示。

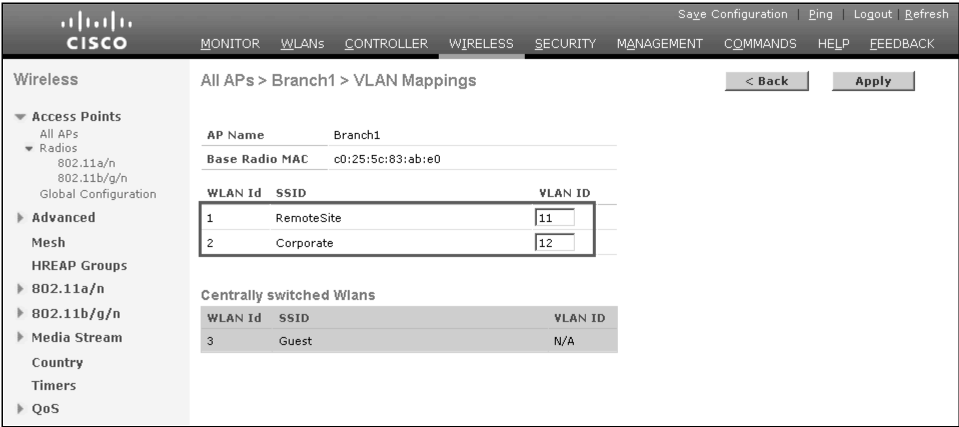


图 4-33　配置 HREAP 上 SSID 对应的 VLAN

⑩ 最后单击 Apply 按钮保存设置。

4.2.4　FlexConnect

在 7.2.103.0 及更高版本的映像软件中，HREAP 被 FlexConnect 取代，在 HREAP 的基础上，FlexConnect 提供了更多的功能和优化。

和 HREAP 组相比，FlexConnect 组增加了更丰富的功能，如图 4-34 和图 4-35 所示。

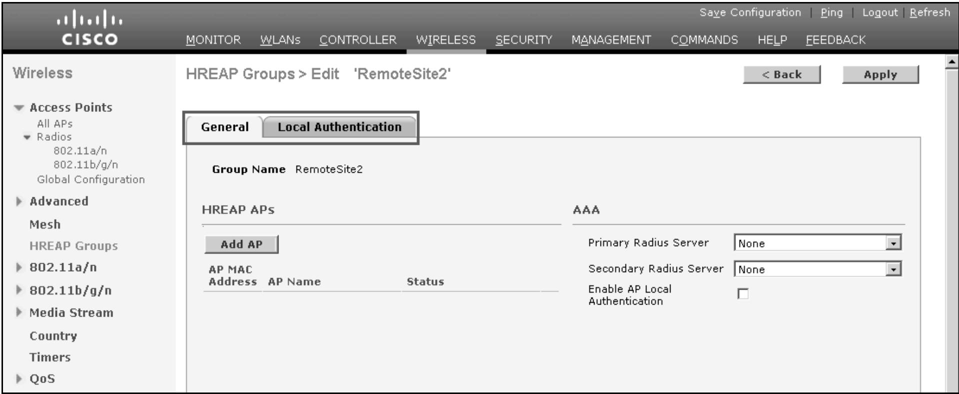


图 4-34　HREAP 组的配置内容

在 Wireless>FlexConnect Groups 页面单击 New 按钮可以创建 FlexConnect 组，然后单击创建的组名称，进入 General 选项卡页面。首先将 FlexConnect AP 加入到组，只需要勾选 Select APs

from current controller，在 AP Name 的下拉框内则会出现配置为 FlexConnect 模式的 AP 名称，单击 Add 按钮添加，如图 4-36 所示。

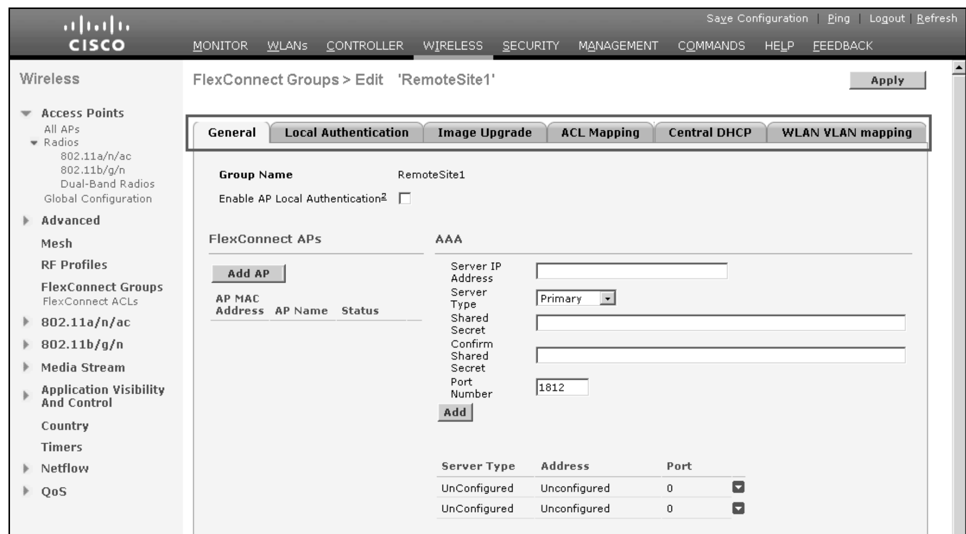


图 4-35 FlexConnect 组的配置内容

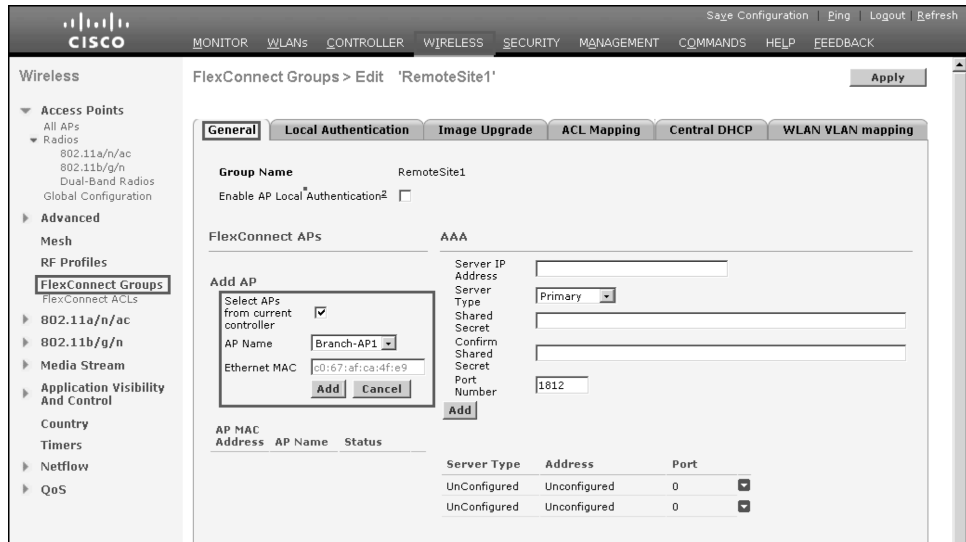


图 4-36 为 FlexConnect 组添加 FlexConnect AP

在 FlexConnect 组中可以配置 AP 的升级策略，能够优化通过 WAN 连接的多个 AP 的镜像软件升级。一般情况下，每个 AP 通过下载 WLC 内的镜像进行升级，还可以利用预下载的特性减少 AP 因升级而不能提供服务的时间。在 FlexConnect 模式中，可以启用更高效的 AP 升级

机制，每种型号的 AP 中都会有一个 Master AP 通过 WAN 率先从 WLC 下载镜像，其他相同型号的 AP 可以通过 LAN 从该 Master AP 下载镜像。选择 Image Upgrade 选项卡，勾选 FlexConnect AP Upgrade 后的复选框，还可以手动选择 Master AP，如图 4-37 所示。

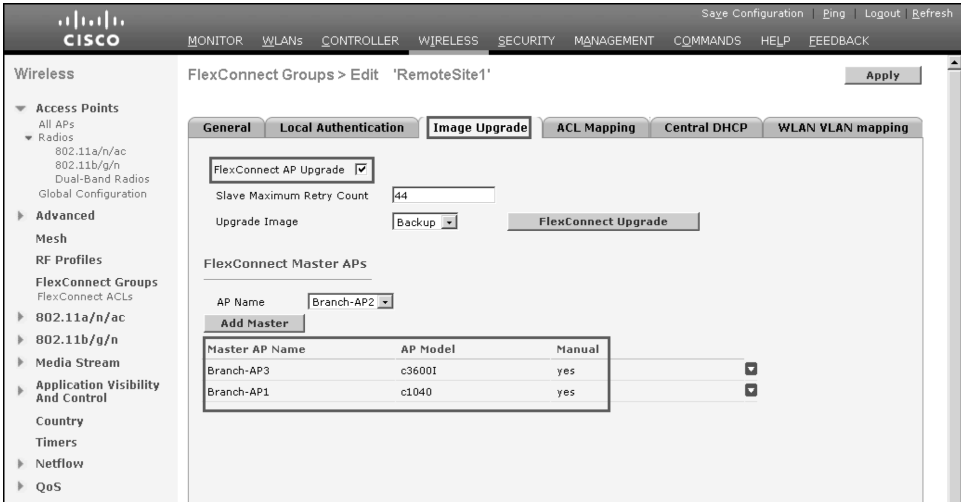


图 4-37　配置高效 AP 升级策略

不同于 HREAP，FlexConnect 组中可以定义 WLAN 和 VLAN 的映射关系，而不必配置每一个 FlexConnect AP，输入 WLAN 的 ID 和 VLAN ID，单击 Add 按钮就可以添加，如图 4-38 所示。

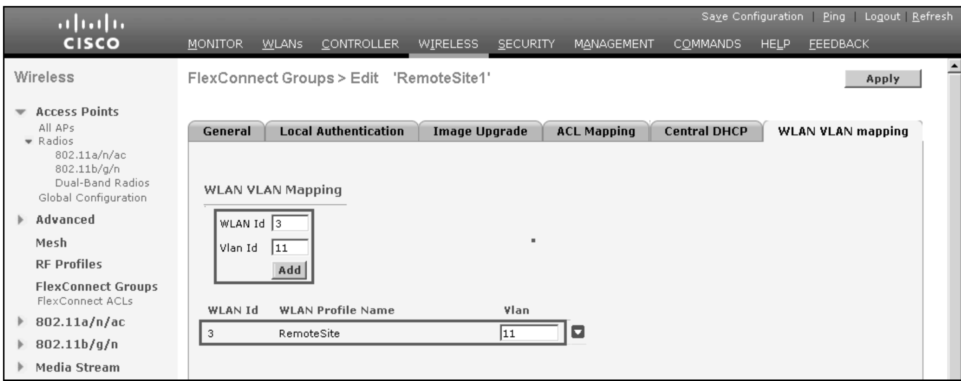


图 4-38　配置 FlexConnect 组的 WLAN 与 VLAN 映射

FlexConnect AP 也可以配置不同的 WLAN 和 VLAN 映射，选择 Wireless>All APs> AP 名称>VLAN Mappings，选中映射关系执行 Make AP Specific，然后在 VLAN ID 输入不同的 WLAN 和 VLAN 映射，如图 4-39 所示。AP 级别的 WLAN 和 VLAN 映射优先于 FlexConnect 组，后者优先于 WLAN 中配置的动态接口所关联的 VLAN。

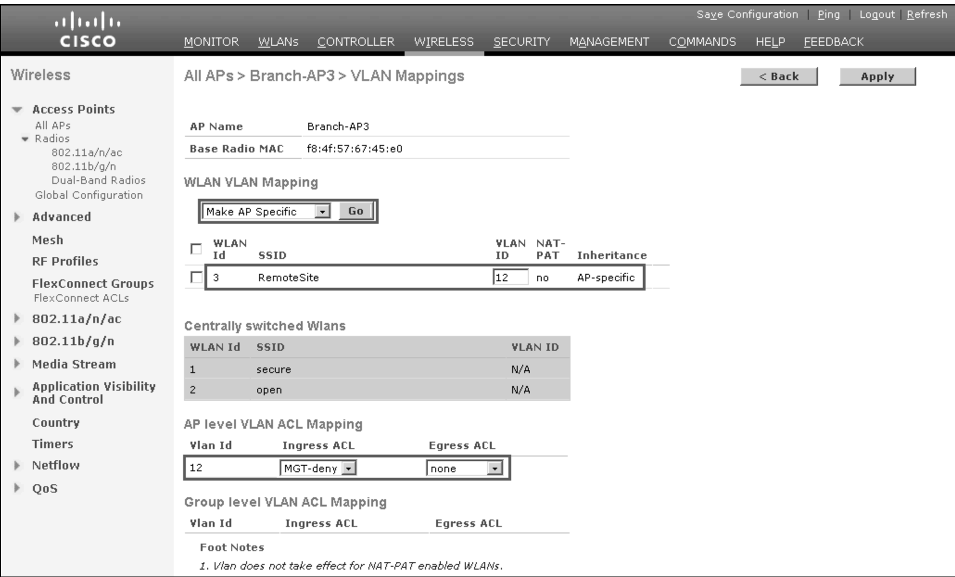


图 4-39　配置 AP 级别的 WLAN 与 VLAN 映射

还可以配置 FlexConnect ACLs，可以分别在 FlexConnect 组级别和 AP 级别对客户端发送和接收的数据进行控制。

4.3　管理无线射频资源

RF 域也称为 RF 组，是除 Mobility Group 以外的另一个重要的部署概念。一个 RF 域就是一系列 WLC 的群，群内的 WLC 在 IEEE 802.11a 及 b/g 的每一个物理信道上互相协调它们的动态射频资源管理（Radio Resource Management，RRM），在 IEEE 802.11 每一个物理频段上都存在一个 RF 域。将 WLC 组成一个 RF 域，允许动态射频资源管理算法在多个 WLC 之间所有的 AP 上具有可扩展性。关于 RRM 的深入研究超出了本书的范围，有兴趣的读者可以参考以下链接：

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml

LAP 会周期性地向空中发送邻居信息，信息中包含了 WLC 的 IP 地址以及关于时间戳和 BSSID 的散列消息完整性检查（Message Integrity Check，MIC）。散列算法使用了在控制器上配置的一个共享密钥，这个密钥通过控制器推送到所有的 AP，所有共享密钥的 AP 可以检查消息的完整性及合法性，如果不同 WLC 上关联的 AP 能够互相之间接收到对方超过−80 dBm 强度的信号，这些控制器之间就会动态地形成一个 RF 组。

RF 域中的成员将会选举一个“领导”负责维持 RF 组内的功率及信道分配方案，主控方将会根据从系统收集到的实时射频资源计算功率，制订信道计划。RRM 的算法一般将 AP 的功率优化在−65 dBm 以下，以消除 IEEE 802.11 信道之间的干扰。

RF 组领导和成员间会以一定的时间间隔（通常为 600 s）相互交换 RRM 信息，在间隔期间，组领导将会发送心跳报文（Keepalive Messages）给每个成员并收集实时的 RF 数据。

WLC 需要配置一个 RF 域的名称参数，同时将这个名称推送到关联到此 WLC 的所有 AP，RF 域的名称将作为 AP 之间共享的密钥用来产生散列的 MIC 邻接报文。一般来说，我们只需将所有的 WLC 上的 RF 域名称设置成一样即可。RF 的域名称通过 Controller>General 页面中的 RF Group Name 修改，如图 4-40 所示。

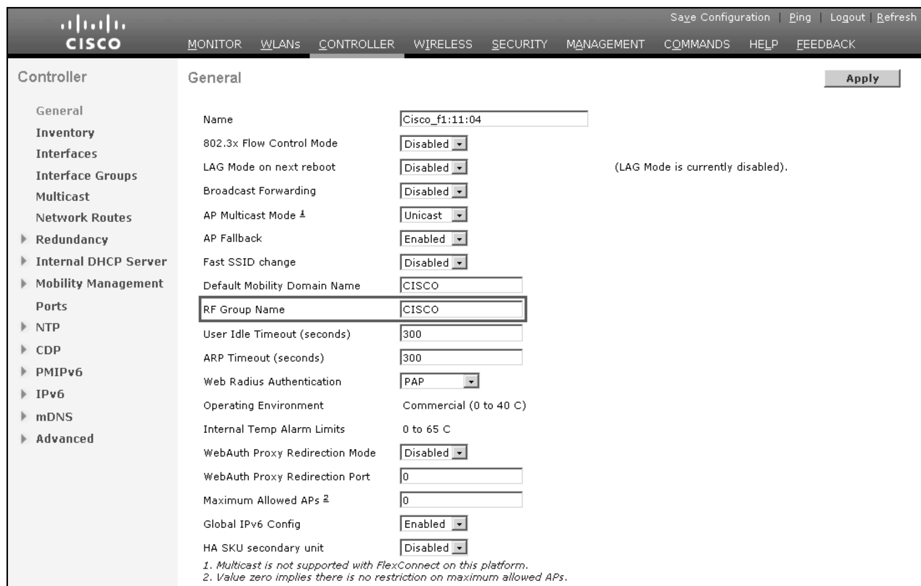


图 4-40　查看和修改 RF 分组名称

RF 组和 Mobility 组外部功能大抵相同，它们都是定义了一个 WLC 的群，但功能不一样，RF 组主要对射频资源进行管理，而 Mobility 是对用户的移动性以及控制器之间的冗余进行管理。

如果加入某个 WLC 的 LAP 收到了来自与其他 WLC 相关联的 LAP 的 RF 信号，这些 WLC 必须被配置在同一个 RF 组中，倘若 AP 之间可以互相侦听到传输信号，那么系统需要配置多个系统间的 RRM，以消除 IEEE 802.11 之间的干扰。此外，如果 AP 收到了其他 AP 的通告信息但无法通过共享的密钥解开，那么其他的 AP 将会被标识为非法（Rogue）的 AP，并在 WLC 中产生一条警告信息，为了防止合法的 AP 被标识为非法 AP，建议将所有的 WLC 都设置在一个 RF 组内。

可以在 WCS 中查看 RF 组的状态信息，转到 Monitor>Controllers，打开相应的 WLC，在左侧的菜单选择 IEEE 802.11a/n 或 IEEE 802.11b/g/n 下的 RRM Grouping，就可以查看当前的 RF 状态，如图 4-41 所示。

显示的信息包括 WLC 是否在已知的物理信道上支持自动分组、组领导者的 MAC 地址、此 WLC 是否为组领导者、最近的更新时间、更新的时间间隔及组中的成员信息等。

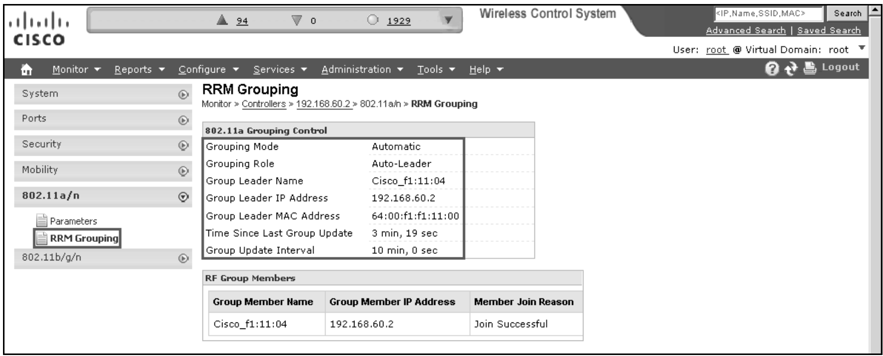


图 4-41　查看 RF 当前状态

4.3.1　重写自动 RF 分组

我们可以重写动态 RRM 的设置而不需要禁止自动 RF 分组功能，这可以通过 WLC 的 Web 管理界面或 WCS 进行。

1．在 WCS 中关闭自动 RF 分组功能

转到 Configure>Controllers，并选择相应的 WLC 打开，在左侧选择 IEEE 802.11a/n 或 IEEE 802.11b/g/n，选择 RRM 下的 RF Grouping 菜单，在右侧的 Grouping Mode 下拉菜单中选择 Off 并保存，即可关闭自动分组功能，如图 4-42 所示。

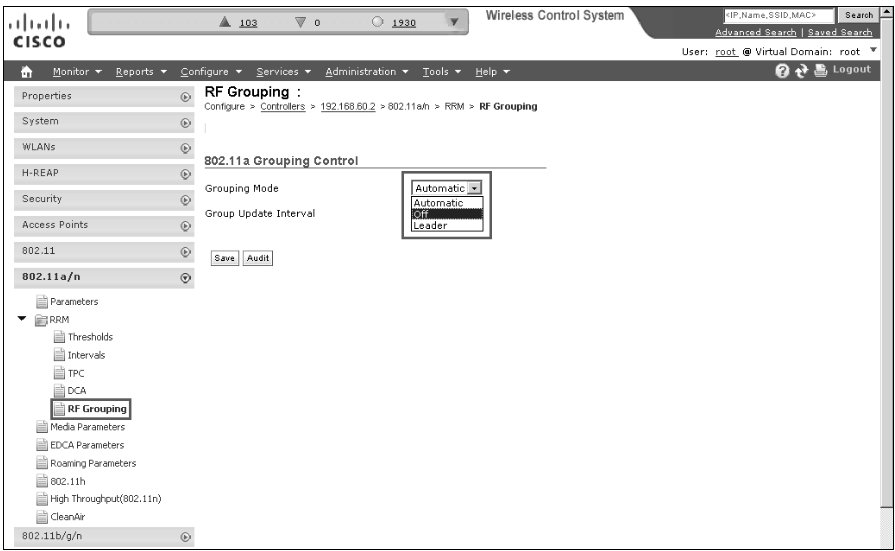


图 4-42　在 WLC 中关闭 RF 自动分组功能

2．在控制器的 Web 管理界面中关闭 RF 自动分组功能

转到 Wireless> IEEE 802.11a/n/ac 或 IEEE 802.11b/g/n>RRM>RF Grouping，在右侧 Group Mode 的下拉框中选择 off 并单击 Apply 按钮，即可关闭 RF 自动分组功能，如图 4-43 所示。

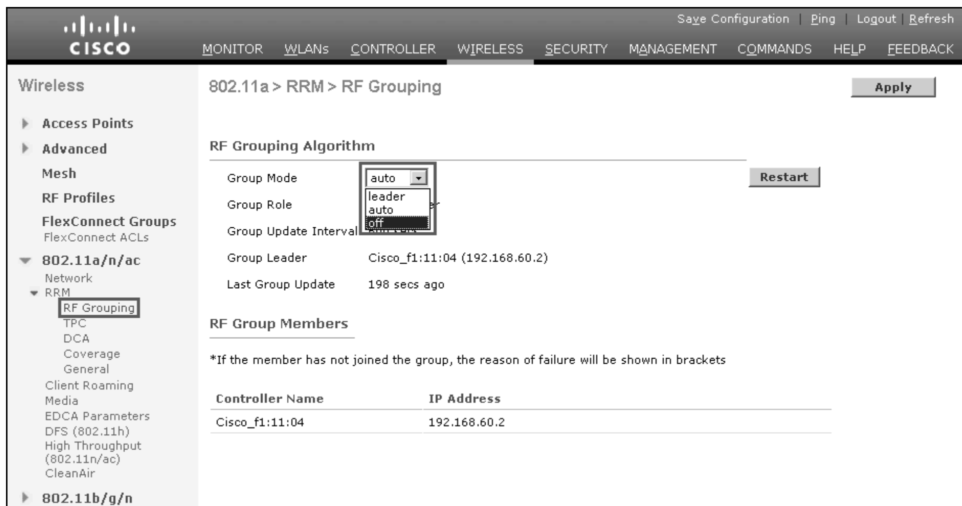


图 4-43　在 WLC 的 Web 管理界面中关闭 RF 自动分组功能

4.3.2　重写动态 RRM

在一些部署中，可能希望静态分配 AP 的信道或者功率，一般来说，我们不建议这么做。即使选择静态分配功率和信道，最好使用自动 RF 分组来避免产生伪非法 AP 事件。可以在 WLC 上关闭全局的信道和功率分配，也可以保留全局自动分配，但针对个别 AP 进行重写。可以通过 WCS 的模板或者 WLC 的 Web 管理接口完成更改。

1．采用 WCS 模板静态更改 AP 的信道及发射功率

选择 Configure> AP Configuration Templates>Lightweight AP，在右上角的命令列表中选择 Add Template，并单击 GO 提交，接下来为 Template 命名并保存。

在接下来的页面中，选择 IEEE 802.11a/n 或 IEEE 802.11b/g/n 选项卡，选中 Channel Assignment 和 Power Assignment 边上的复选框，并选择 Custom 的选项，可以分别指定信道以及功率信息，如图 4-44 所示。设置完成后，选择 Select APs 选项卡，并在选择相关的 AP 后选择 Apply/Schedule 选项卡，立即应用设置或放入任务计划。

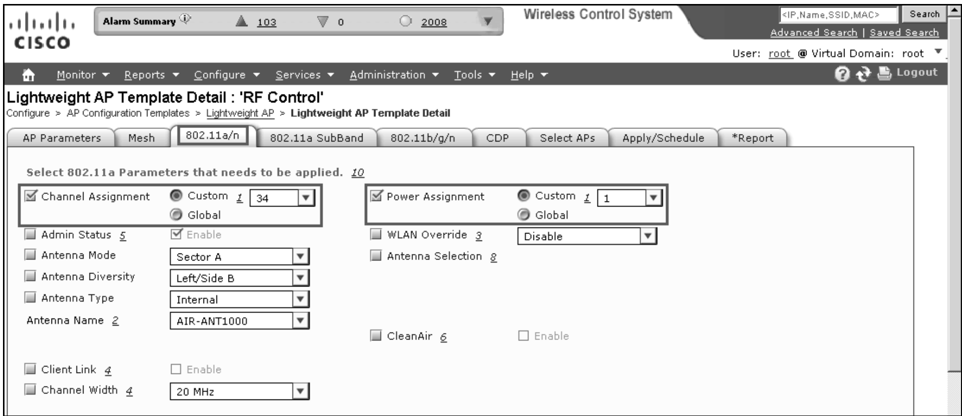
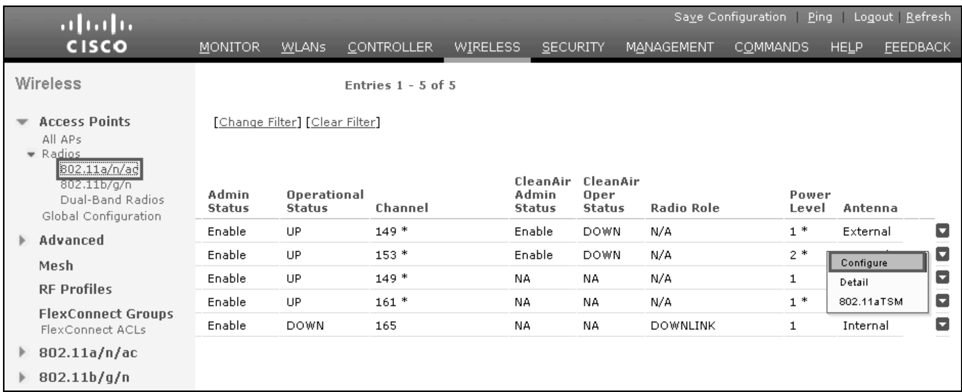


图 4-44 在 WCS 中手动分配信道及发射功率

2．采用 WLC 的 Web 管理接口配置

导航到 Wireless>Access Points>All APs，选择 IEEE 802.11a/n/ac 或 IEEE 802.11b/g/n 任一种物理方式，在 AP 列表中选择需要配置的 AP，从右侧蓝色的图标中选择 Configure，如图 4-45 所示。



Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Radio Role	Power Level	Antenna
Enable	UP	149 *	Enable	DOWN	N/A	1 *	External
Enable	UP	153 *	Enable	DOWN	N/A	2 *	
Enable	UP	149 *	NA	NA	N/A	1	
Enable	UP	161 *	NA	NA	N/A	1 *	
Enable	DOWN	165	NA	NA	DOWNLINK	1	Internal

图 4-45 在 WLC 的 Web 界面中查看 AP 的 RRM 信息

在配置页面的 RF Channel Assignment 下的 Assignment Method 中选择 Custom 就可以自定义信道，同样，在 Tx Power Level Assignment 下的 Assignment Method 中选择 Custom 也可以自定义发射功率的等级，设置完成后单击 Apply 按钮，如图 4-46 所示。

4.3.3 频段选择

2.4 GHz 频段只有 3 个不重叠的信道，通常很拥挤，还会受到蓝牙、微波炉、无绳电话等

的干扰。频段选择功能通过延迟 2.4 GHz 的探查请求，可以使支持双频（2.4 GHz 和 5 GHz）的客户端优先使用 5 GHz 连接 AP。

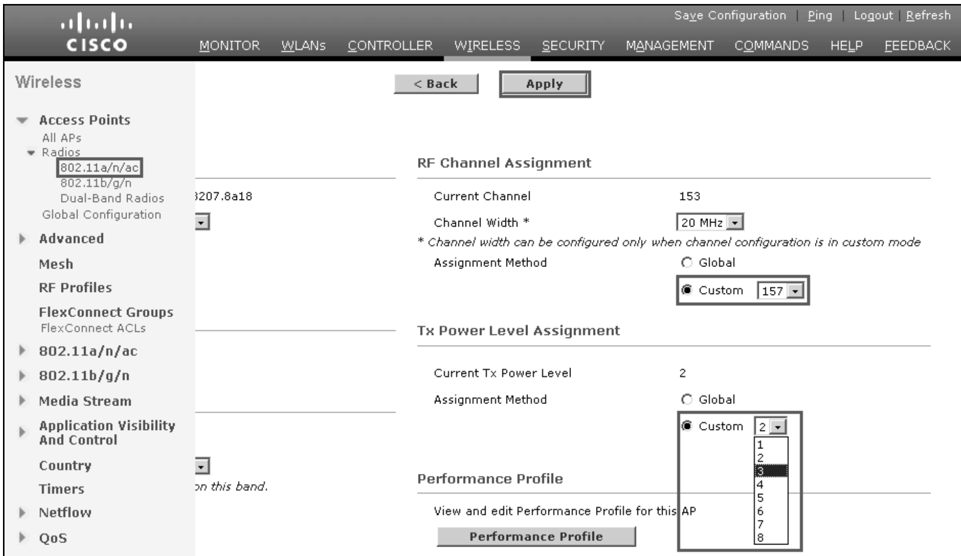


图 4-46　在 WLC 的 Web 界面中手工分配信道及功率

频段选择功能仅支持 Cisco Aironet 1040、1140、1250、1260、3500 和 3600 系列的 AP。启用频段选择功能的 WLAN 因为漫游延迟，不支持语音和视频等对时间敏感的应用。

频段选择功能默认是全局启用的，选择 Wireless>Advanced>Band Select 可以查看和配置全局参数，如图 4-47 所示。

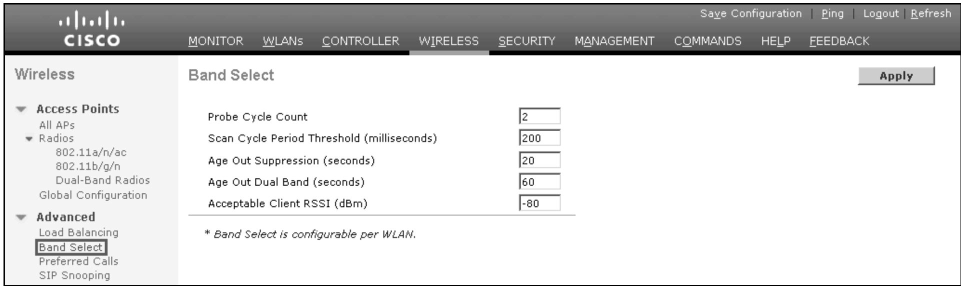


图 4-47　频段选择功能全局参数

在某个 WLAN 中启用频段选择功能，选择 WLANs>WLAN ID，到 WLAN>Edit 页面，点击 Advanced 选项卡，勾选 Client Band Select，如图 4-48 所示。

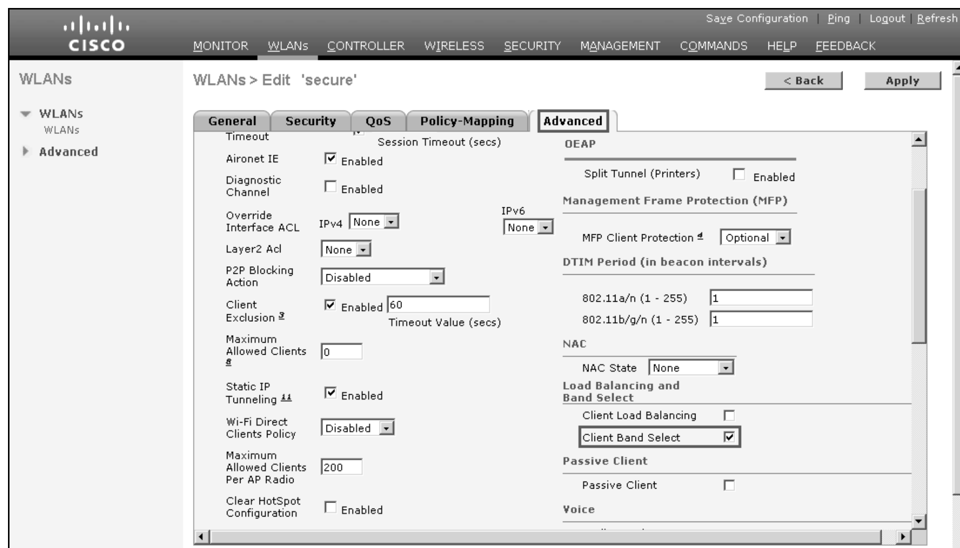


图 4-48　在 WLAN 启用频段选择功能

4.4　配置 IEEE 802.11n 网络

Cisco 802.11n AP（如 1140 系列无线接入点）能够像任何其他轻量级无线接入点一样与无线局域网控制器互操作。只要控制器运行 5.2 或更高版本的映像代码，IEEE 802.11n AP 就可以发现并加入控制器。IEEE 802.11ac AP 除了需要控制器运行 7.6 或更高版本映像代码外，还对控制器型号有要求，如 WiSM、4400 系列和 4100 系列等就不支持 IEEE 802.11ac AP。

4.4.1　启用 IEEE 802.11n 的速率

- 第 1 步：在控制器界面中的“Wireless”标签下，单击“802.11 a/n/ac”或“802.11 b/g/n”的网络设置。
- 第 2 步：单击“High Throughput (802.11n/ac)”或“High Throughput (802.11n)”，打开配置页。
- 第 3 步：确保“11n Mode”和“11ac Mode”模式已启用。默认情况下，所有的 MCS（或 IEEE802.11n 的数据传输速率）是启用的，如图 4-49 所示。

根据空间流（Spatial Stream，SS）的数量不同，可以选择在 AP 和客户端之间支持的 IEEE 802.11n 速率，其中每种空间流中序号为 8 和 9 的 MCS 专用于 IEEE 802.11ac。

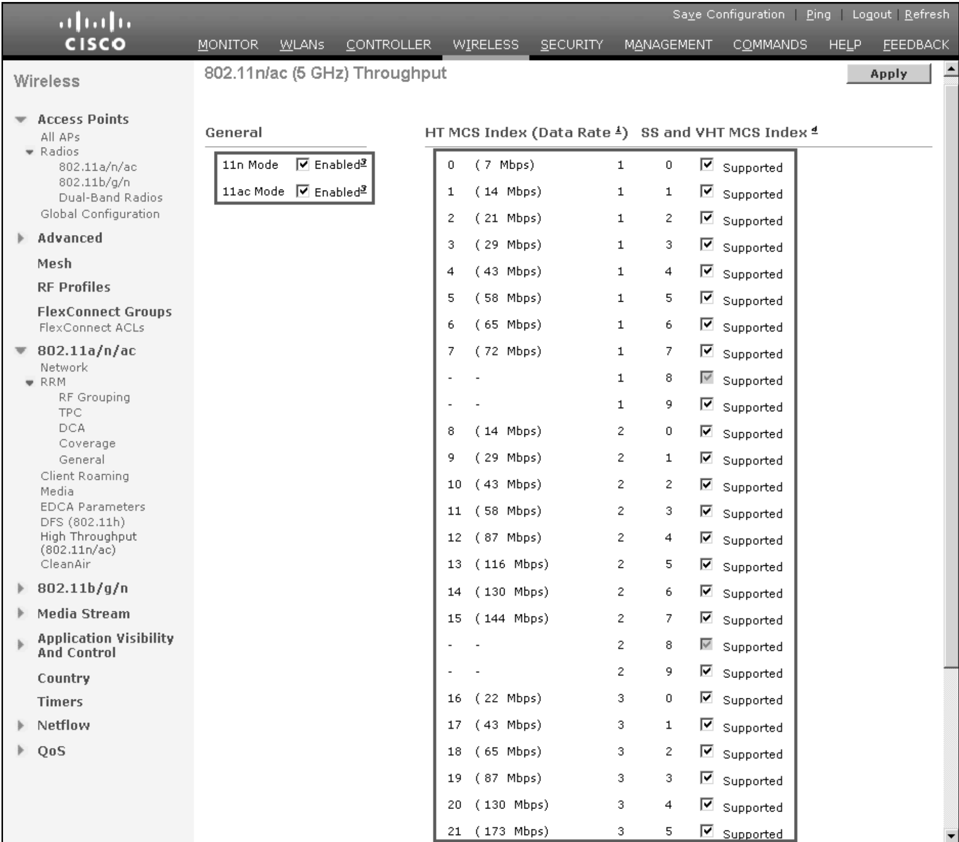


图 4-49　选择 IEEE 802.11n 的速率

4.4.2　配置 IEEE 802.11n 的无线局域网（WLAN）

为了使无线局域网（或 SSID）运行于 IEEE 802.11n 速率，两个具体项目——数据加密和服务质量必须设定。按照 IEEE 802.11n 标准本身的要求，所有的加密链接现在必须使用 AES 加密算法。另外一种连接方式是无线局域网运行在没有加密的状态，这是可能的选择。但是 IEEE 802.11n 标准排除了通过 WEP、TKIP 或任何其他形式的传统加密技术来使用 IEEE 802.11n 的数据传输速率，如图 4-50 和图 4-51 所示。

至于服务质量，无线局域网必须配置为允许 WMM，以便使 IEEE 802.11n 速率可以运行。如果要在无线局域网控制器上设定这个参数，在 WLAN 配置界面下设置 QoS 参数为“Allowed”或“Required”，如图 4-52 所示。

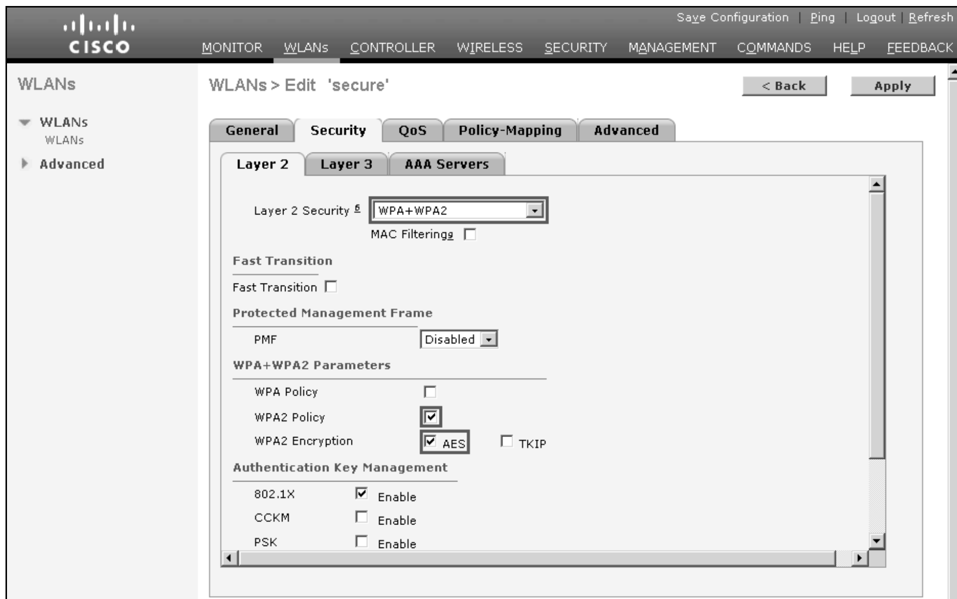


图 4-50 设置“Layer 2 Security”为“WPA2 AES”方式



图 4-51 设置“Layer 2 Security”为“None”

4.4.3 启用数据汇聚

默认情况下，无线局域网控制器启用数据汇聚功能。如果由于某种原因，例如，从先前的软件升级且先前的软件关闭了数据汇聚功能，就需要在控制器上启用该功能。

```
(Cisco Controller)> config 802.11a network disable
(Cisco Controller)> config 802.11a 11nSupport a-mpdu tx priority 0 enable
(Cisco Controller)> config 802.11a network enable
(Cisco Controller)> config 802.11b network disable
```

```
(Cisco Controller)> config 802.11b 11nSupport a-mpdu tx priority 0 enable
(Cisco Controller)> config 802.11b network enable
```

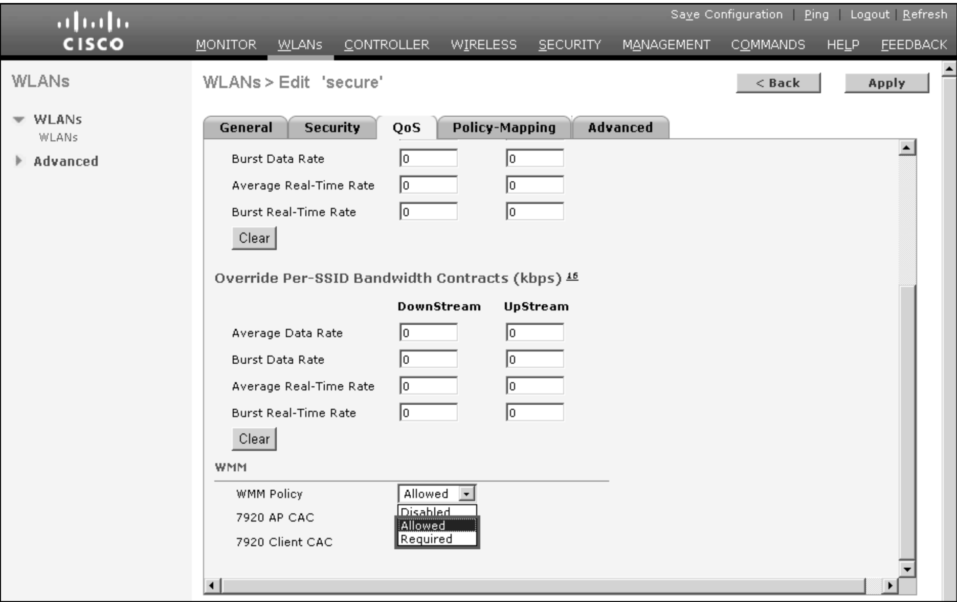


图 4-52　设置“WMM Policy”　为“Allowed”或“Required”

确认数据包汇聚已启用：

```
(Cisco Controller)> show 802.11a
802.11n Status:
A-MPDU Tx:
Priority 0............................... Enabled
Priority 1............................... Disabled
Priority 2............................... Disabled
Priority 3............................... Disabled
Priority 4............................... Disabled
Priority 5............................... Disabled
Priority 6............................... Disabled
Priority 7............................... Disabled
```

4.4.4　40 MHz 和 80 MHz 频宽操作

要达到 IEEE 802.11n 支持的最大吞吐量，需要利用 40 MHz 频宽信道才能实现。在这种模式下，两个传统的和连续的 20 MHz 信道绑定在一起共同创建了一个双倍宽度的信道，从而使

性能加倍。由于 5 GHz 频段可用频谱数量大幅增加，建议在这个频段使用 40 MHz 频宽的信道。至于 2.4 GHz 频段，由于这一频段可用的频谱十分有限，建议放弃 40 MHz 频宽的操作。总之，只能在 5 GHz 频段使用 40 MHz 频宽的信道。在控制器上配置 40 MHz 频宽有两种机制：通过使用无线资源管理来自动分配信道，或静态配置接入点无线射频模块工作的信道。

对于 IEEE 802.11ac，还可以利用 80 MHz 频宽信道，这样可以在 5 GHz 频段上将连续的 4 个 20 MHz 信道绑定在一起，大幅提高传输速率。

注意

您可以在 1140 系列无线接入点的 2.4 GHz 无线电模块上配置 40 MHz 频宽的信道，但这是严重不推荐的！反对的主要理由是，2.4 GHz 频段频谱有限，且干扰众多，性能问题经常发生。在 2.4 GHz 频段上配置 40 MHz 频宽的信道仅通过静态方式完成，而不是通过无线资源管理自动分配的。

4.4.5 使用无线资源管理

无线资源管理（RRM）可以用来为 IEEE 802.11n 接入点自动选择 40 MHz 信道，同样也可以为 IEEE 802.11ac 接入点自动选择 80 MHz 信道，对于不支持 IEEE 802.11ac 的 IEEE 802.11n 接入点则自动使用 40 MHz 信道，因此可以配置频宽为 80 MHz。配置这一功能的具体操作为：首先在 Wireless> IEEE 802.11a/n/ac>Network 配置页，将 IEEE 802.11a Network Status 的 Enable 复选框勾除，单击 Apply，然后在“Wireless> IEEE 802.11a/n/ac > RRM > Dynamic Channel Assignment（DCA）”配置页，将“Channel Width”的配置从“20 MHz”改变为 “80 MHz”，单击 Apply 按钮，如图 4-53 所示。修改频宽配置后再将 IEEE 802.11a Network Status 的 Enable 复选框勾中，单击 Apply。

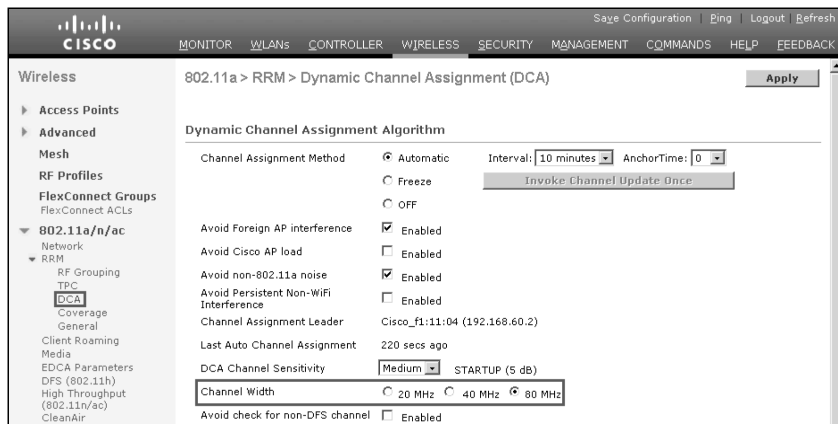


图 4-53 在 80 MHz 频宽上配置使用无线资源管理

通过 Wireless>Access Points>Radios> IEEE 802.11a/n/ac 可以看到 DCA 为 AP 自动分配的信道，如图 4-54 所示。

802.11a/n/ac Radios　　Entries 1 - 5 of 5

Current Filter: None　　[Change Filter] [Clear Filter]

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Radio Role	Power Level	Antenna
APb838.612d.4f80	1	b8:38:61:4a:36:80	-	Enable	UP	(149,153,157,161) *	Enable	DOWN	N/A	1 *	External
AP4c4e.3546.f372	1	20:bb:c0:72:2b:90	-	Enable	DOWN	165	NA	NA	DOWNLINK	1	Internal
APc067.afca.4fe9	1	c0:25:5c:83:97:a0	-	Enable	UP	(157,161) *	NA	NA	N/A	1 *	Internal
AP4c00.8207.8a18	1	f8:4f:57:84:ba:40	-	Enable	UP	(149,153) *	Enable	DOWN	N/A	2 *	Internal
AP1	1	0c:d9:96:4d:91:90	-	Enable	UP	(157,161) *	NA	NA	N/A	1	Internal

* global assignment

图 4-54　80MHz 频宽配置结果验证

4.4.6　使用静态无线资源管理

40 MHz 和 80 MHz 频宽信道也可以静态配置在无线接入点上，配置的方法和 20 MHz 频宽信道一样。在图 4-55 的截图中，IEEE 802.11 a/n 模块上配置为工作在信道 157 且信道宽度为 40 MHz。虽然实际的信道选择在此的配置是 157 ，事实上，是利用信道 157 和信道 161 两个信道创造了一个 40 MHz 频宽的信道。在图 4-55 中，“Current Channel”选项里就显示了这两个控制和扩展信道的使用。

802.11a/n Cisco APs > Configure　　< Back　Apply

General

AP Name	APb838.612d.4f80
Admin Status	Enable
Operational Status	UP
Slot #	1

11n Parameters

11n Supported	Yes

RF Channel Assignment

Current Channel	(157,161)
Channel Width *	40 MHz

* Channel width can be configured only when channel configuration is in custom mode

Assignment Method	Global
	Custom 157

Tx Power Level Assignment

Current Tx Power Level	1

图 4-55　在 40 MHz 频宽上配置使用静态无线资源管理

当选择了一个静态分配的 40 MHz 频宽信道时，无线电模块会自动选择适当的扩展（或相邻信道）与其进行绑定。在上面的例子中，信道 157 被选中，那么信道 161 自动被用作扩展信道。另一个例子是，如果选择了信道 149，信道 153 将被选定为扩展信道。这适用于所有 5 GHz 频段的信道在设定为 40 MHz 频宽时的操作，只有相邻信道可以被绑定。

支持 IEEE 802.11ac 的 AP 可以选择 80 MHz 频宽信道，例如，当信道 149 被选中时，那么信道 153、157、161 会被用作扩展信道，如图 4-56 所示。

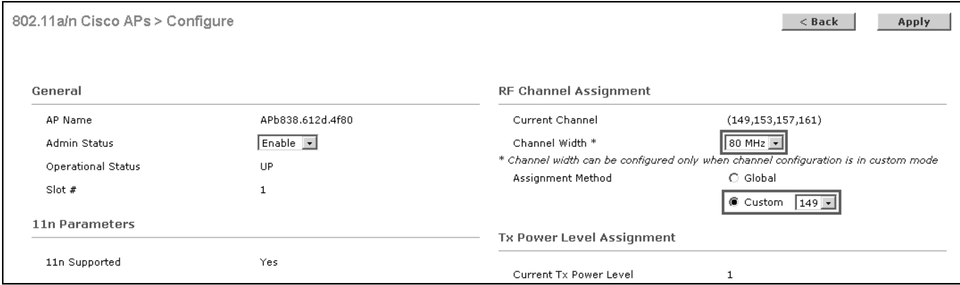


图 4-56　在 80 MHz 频宽上配置使用静态无线资源管理

4.4.7　确认 IEEE 802.11n 和 IEEE 802.11ac 网络已运行

在确保 WLAN 基础设施具有适当的 IEEE 802.11n 和 IEEE 802.11ac 运行配置后，确认客户端是否采用 IEEE 802.11n 或 IEEE 802.11ac 标准的高速率连接也很简单。可在无线局域网控制器的图形用户界面单击“Monitor”，然后单击“Client”就可检查客户端的运作模式。在图 4-57 的截图中，每个客户端的协议项显示了客户端使用的连接类型。对于 IEEE IEEE 802.11n 的连接方式，如果显示为“802.11an”，则意味着一个 5 GHz 频段的 IEEE IEEE 802.11n 连接；如果显示为“802.11ac”，则意味着一个 5 GHz 频段的 IEEE 802.11ac 连接；如果显示为“802.11bn”，则表示一个 2.4 GHz 频段的 IEEE 802.11n 连接。

Clients　　Entries 1 - 3 of 3

Current Filter　None　[Change Filter] [Clear Filter]

Client MAC Addr	IP Address	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth
08:57:00:0a:83:c3	10.4.4.11	APb838.612d.4f80	secure	secure	Unknown	802.11bn	Associated	Yes
0c:82:68:54:65:ac	10.4.4.12	APb838.612d.4f80	secure	secure	Unknown	802.11an	Associated	Yes
d4:97:0b:4c:2d:24	10.4.4.10	APb838.612d.4f80	secure	secure	Unknown	802.11ac	Associated	Yes

图 4-57　确认 IEEE 802.11n 正常运行

4.5　配置 Cisco Wireless Mesh 网络

无线 Mesh 网络是一种新的无线局域网类型，与传统的 WLAN 不同的是，无线 Mesh 网络中的 AP 是无线连接的，而且 AP 间可以建立多跳的无线链路。无线 Mesh 网络只是对骨干网进行了变动，和传统的 WLAN 没有任何区别，无线 Mesh 技术使得管理员可以轻松地部署质优价廉的无线局域网。无线 Mesh 网络的优点如下所述。

（1）高性价比

在无线 Mesh 网络中，只有 RAP（Root Access Point）需要接入有线网络，对有线的依赖

程度被降到了最低程度，省去了购买大量有线设备及布线安装的投资开销。

（2）可扩展性强

在无线 Mesh 网络中，AP 之间能自动相互发现并发起无线连接建立，如果需要向网络中增加新的 AP 节点，只需要安装新增节点并进行相应的配置。

（3）部署快捷

组建无线 Mesh 网络，除 RAP 外的其他 AP 均不需要走线接入有线网络，和传统 WLAN 网络相比，大大缩短了组建周期。

（4）应用场景广

无线 Mesh 网络除了可以应用于企业网、办公网和校园网等传统 WLAN 网络常用场景外，还可以广泛应用于大型仓库、港口码头、城域网、轨道交通和应急通信等应用场景。

（5）高可靠性

在传统 WLAN 网络模式下，一旦某个 AP 上行有线链路出现故障，则该 AP 所关联的所有客户端均无法正常接入 WLAN 网络。而无线 Mesh 网络中各 AP 之间实现的是全连接，从某个无线 Mesh AP 至 RAP 的网络通常有多条可用链路，可以有效避免单点故障。

4.5.1　思科 Mesh 无线架构

在 Cisco 统一无线网络中，所有的 MESH AP 可以分为两种：Root Access Point （RAP）和 Mesh Access Point（MAP）；RAP 使用有线同控制器相连，MAP 通过无线链路最终同控制器相连。MAP 之间相互通信并最终通过 RAP 将数据送回到控制器，MAP 之间使用 AWPP（Cisco Adaptive Wireless Path Protocol）来决定 MAP 到控制器的最佳传输路径。图 4-58 显示了 RAP 同 MAP 之间的联系。

无线 Mesh 网能够同时携带两种类型的流量：WLAN 客户端的数据和 MAP 以太网端口的流量。WLAN 客户端的流量在控制器上终结，以太网流量在 MAP 的以太网端口上终结。MAP 采用如下的两种方式接入到无线 Mesh。

- MAC 认证：将 MAP 的 MAC 地址加入数据库中以便允许 MAP 关联到指定的控制器；
- 外部 RADIUS 认证：MAP 可以通过外部的 RADIUS 服务器授权来关联到指定的服务器。

Mesh AP 支持如下几种部署方式。

① Wireless Mesh；

② WLAN Backhaul（回程）；

③ 点对多点无线桥接；

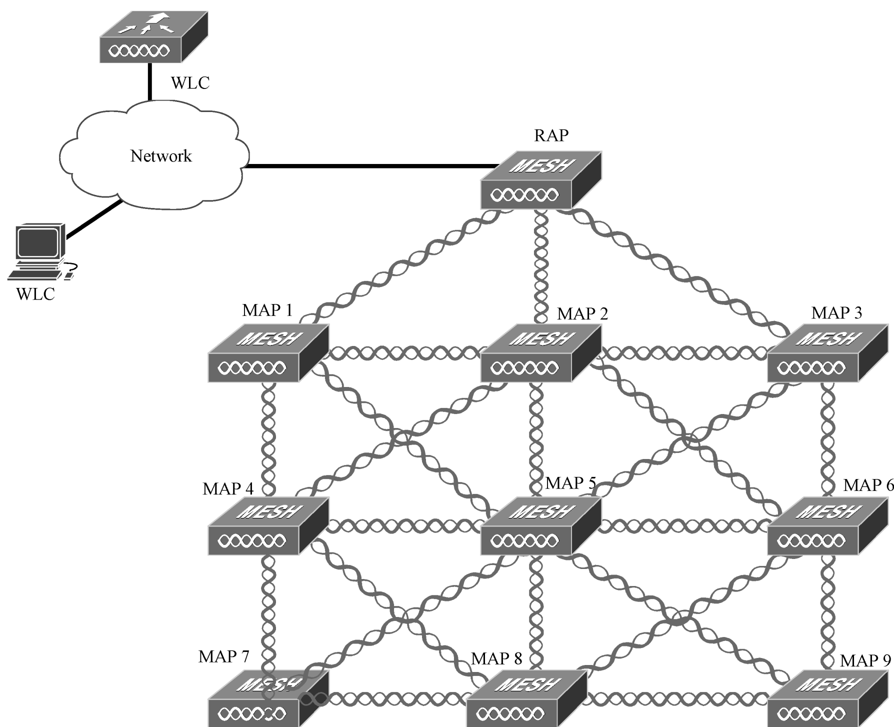


图 4-58　RAP 与 MAP

④ 点对点无线桥接。

在 Cisco 室外 Mesh 网络中，多个 Mesh AP 组成了一个网络，提供安全。可扩展的室外无线局域网部署结构如图 4-59 所示。

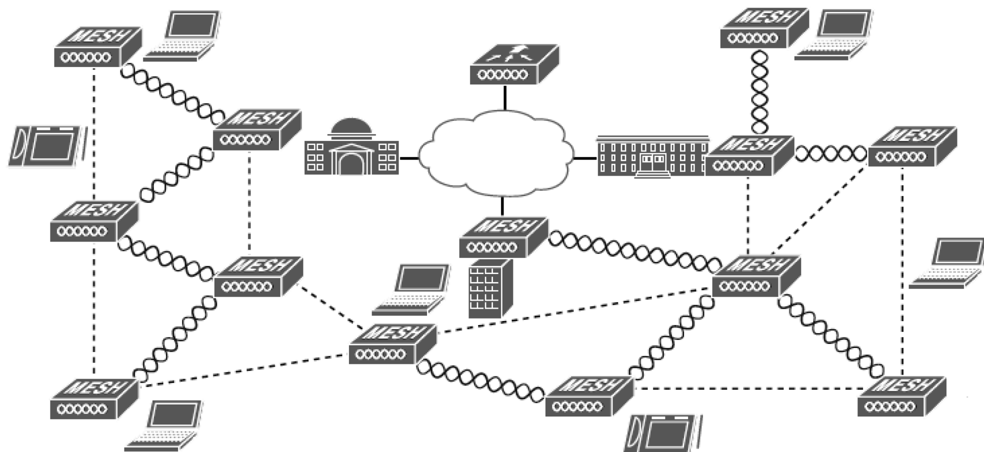


图 4-59　室外 Mesh AP 的部署

Mesh AP 可以提供一个简单的无线回传路径，以便使用 IEEE 802.11a/b/g 为无线及有线用户提供网络服务，在这种情况下，通常只有一个 MAP，图 4-60 表示了这样一个通过 MAP 接入为无线及有线用户提供网络服务的例子。

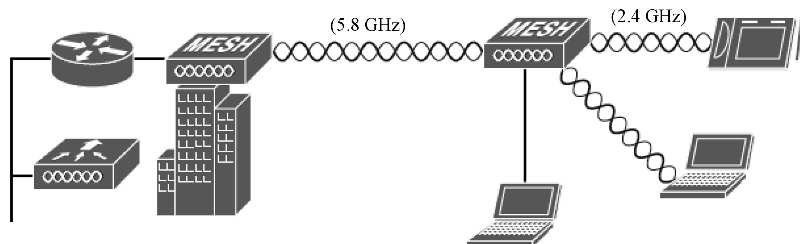


图 4-60　使用无线回传

Mesh AP 还支持点对点桥接应用，在这种部署中，Mesh AP 通过使用回传信号将两个办公场所连接起来，通过这种方式扩展了第二层的网络，这种基础的 Mesh 网只有一个 MAP 并没有无线客户端。

桥接方式也可以允许客户端接入，然而如果在大楼之间桥接，MAP 安装在大楼顶上，可能不适合作为用户接入点。如果使用以太网桥接功能，必须在 RAP 及所有的 MAP 上开启桥接功能，在采用桥接功能时，确认交换机连接 MAP 的端口没有使用 VTP 协议，否则有可能导致 RAP 无法连接控制器，如图 4-61 所示。

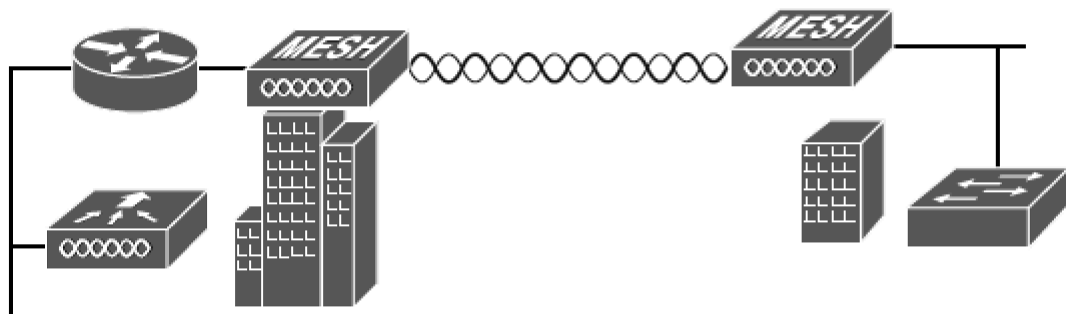


图 4-61　无线点对点的桥接部署

Mesh AP 支持点对多点的桥接应用，RAP 用作根，建立同多个 MAP 的连接，MAP 使用有线同以太网相连。默认情况下，MAP 上的桥接功能是被禁止的，如果使用以太网桥接功能，必须在控制器上对每个 MAP 开启对 RAP 的桥接功能，如图 4-62 所示。

自适应无线路径协议（Adaptive Wireless Path Protocol，AWPP）是 Cisco 为无线 Mesh 网定制的路由协议，AWPP 的路径选择基于链路的质量及跳数。为了部署方便，快速覆盖，最少的资源消耗也是 AWPP 的核心组件。AWPP 的目标是为每个 MAP 找到连接 RAP 的最佳路径，为了实现这个目标，MAP 将主动向邻居 MAP 发起轮询，在轮询期间，MAP 得到了所有的邻居

通向 RAP 的路径，通过比较，决定最好的路径，然后保持同那个 MAP 同步。

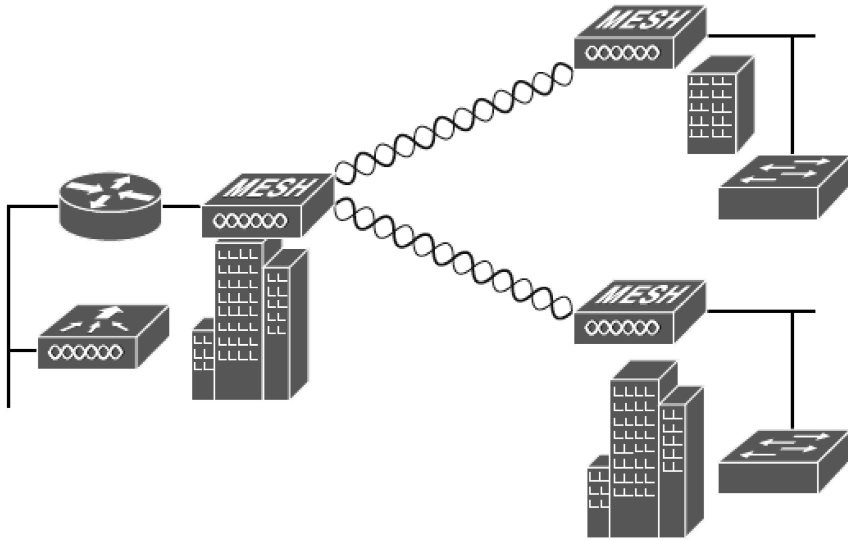


图 4-62　点对多点的桥接部署

下面介绍 Mesh AP 的邻居、父亲和孩子节点。

Mesh AP 之间的关系可以标记为父亲（Parent）、孩子（Child）和邻居（Neighbor）节点。一个父亲 AP 提供了最好的通向 RAP 的路径，父亲节点可以是 RAP，也可以是另一个 MAP。路径的计算使用 SNR 和链路的跳数。孩子 AP 使用父亲 AP 作为通向 RAP 的最佳路径。邻居 AP 是在其 RF 覆盖范围以内的 AP，是没有被选择为父亲和孩子节点的 AP，如图 4-63 所示。

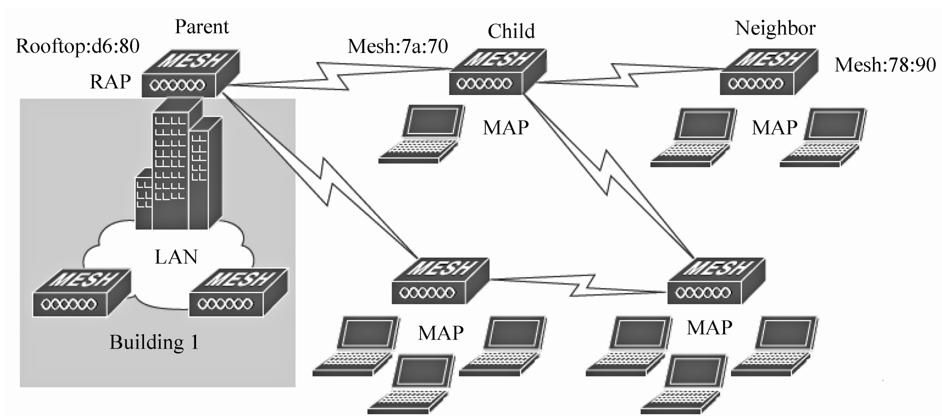


图 4-63　Parent、Child 和 Neighbor AP

4.5.2　在网络中增加 Cisco Mesh AP

向 Cisco 的 Mesh 网络中增加 Mesh AP 之前需要将 Mesh AP 的 MAC 地址加入控制的过滤列表中，其步骤如下所述。

① 导航到 Security > AAA > MAC Filtering 页面中，如图 4-64 所示。

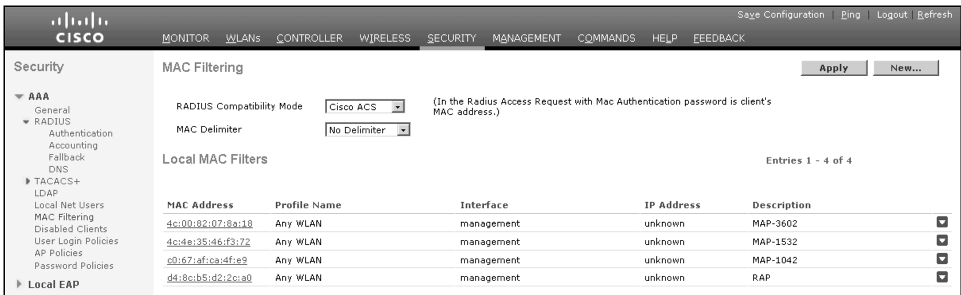


图 4-64　配置 Mesh AP 的 MAC 地址过滤

② 选择 NEW，打开输入 MAC 地址窗口，在 MAC 地址框中，输入 Mesh AP 的 MAC 地址，如图 4-65 所示。



图 4-65　为 Mesh AP 建立配置文件

对于 1522 和 1524/1524SB 的室外 Mesh AP，输入 BVI 的 MAC 地址作为过滤地址；对于 1130 和 1240 的室内 Mesh AP，输入 AP 以太网口的地址；如果无法在外壳上查找 MAC 地址，使用命令 sh int | i Hardware 查找 BVI 或 MAC 地址。

③ 从 Profile Name 的下拉列表中选择 Any WLAN。

④ 从 Interface Name 的下拉列表中选择连接控制器连接 AP 的端口。

⑤ 单击 Apply 应用设置。

4.5.3　配置 Mesh AP 的桥接模式

1500 系列的 Mesh AP 出厂时都被配置为 MAP，不需要修改桥接模式，而加入到网络中的

其他系列的 Mesh AP 必须将 AP 模式更改为桥接模式才能建立无线 Mesh 网络，其设置步骤如下所述。

① 导航到 Wireless>Radios>802.11a/n/ac，在蓝色下拉框选择 Configure，如图 4-66 所示。

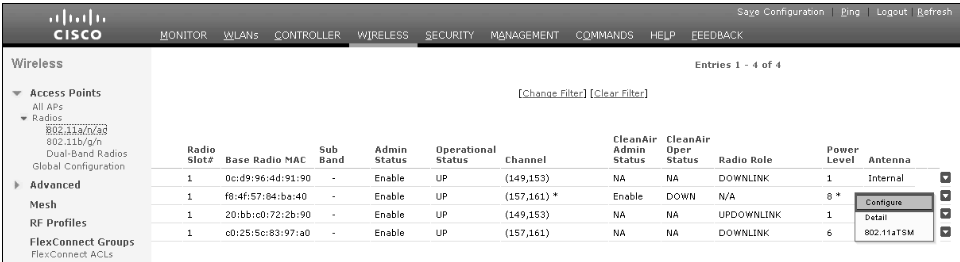


图 4-66　导航到 AP 参数配置界面

在 802.11a/n Cisco APs>Configure 界面，将信道和发射功率配置为 Custom，如图 4-67 所示。

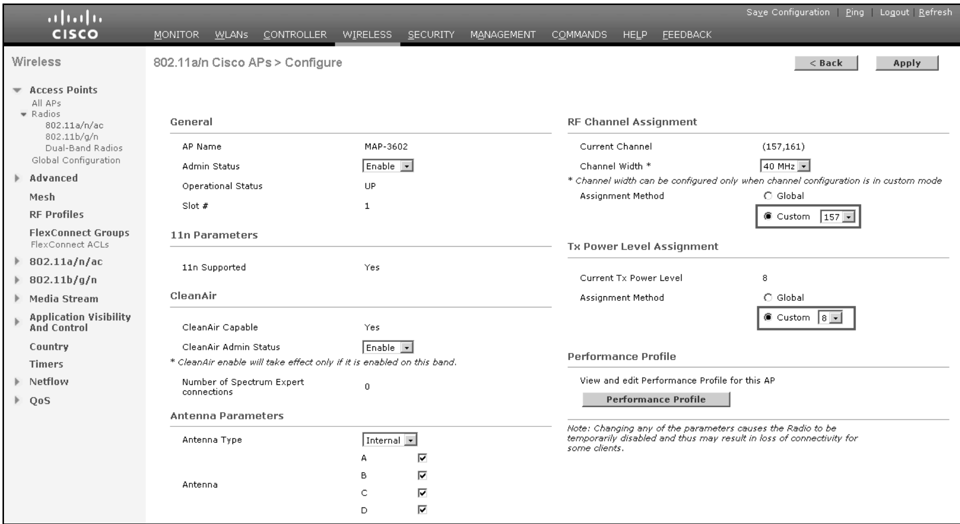


图 4-67　配置 Mesh AP 的信道和发射功率

② 导航到 Wireless 以打开所有的 AP 信息，单击 AP 的名称以打开 AP 的详细信息，如图 4-68 所示。

③ 为了配置 Mesh AP 必须首先将 AP 的模式更改为 Bridge 模式，在 AP Mode 下拉列表中选择 Bridge。

④ 单击 Apply 应用设置。

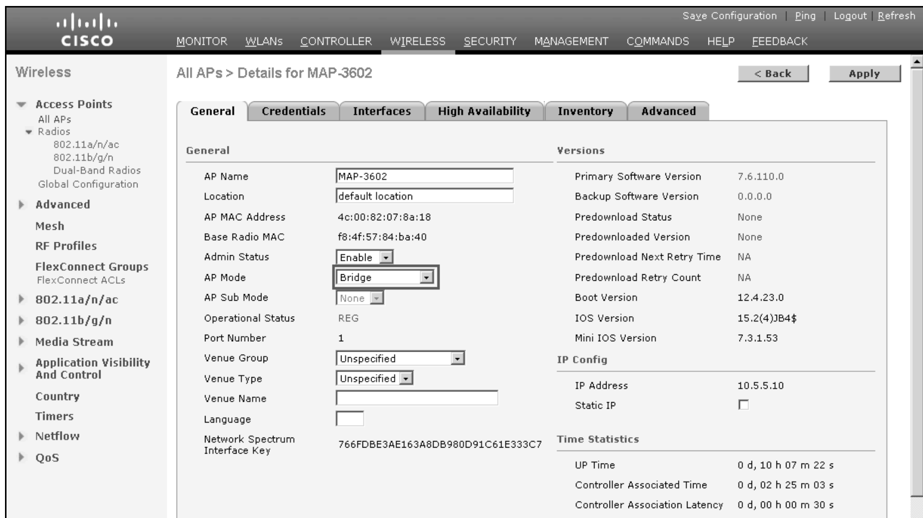


图 4-68　配置 Mesh AP 的模式

4.5.4　配置 Mesh AP 的角色

加入网络的 Mesh AP 需要配置其角色，以设定其为 RAP 或 MAP，设置步骤如下所示。

① 导航到 Wireless，打开所有的 AP 列表。

② 单击需要设置的 AP 名称，出现 All APs > Details for AP 名称页面。

③ 单击 Mesh 标签，如图 4-69 所示。

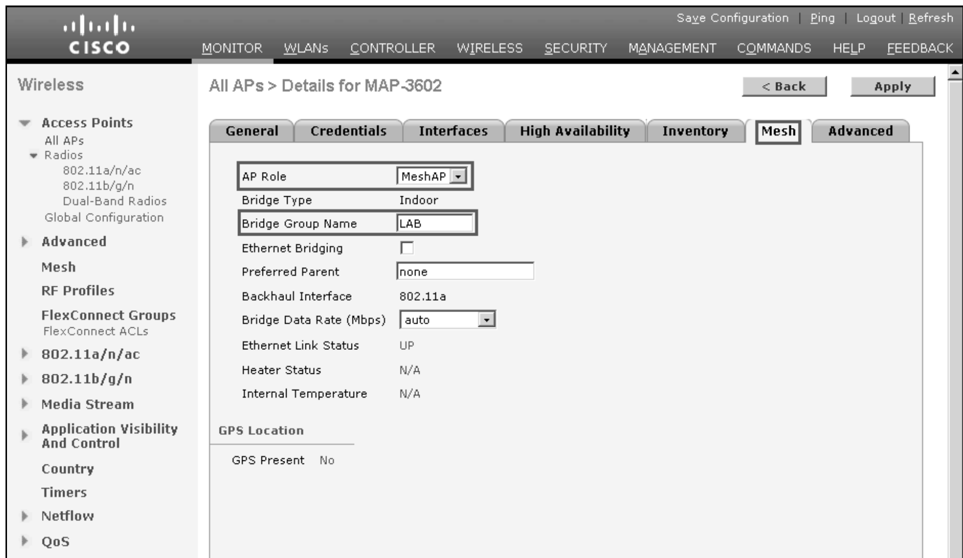


图 4-69　配置 Mesh AP 的角色

④ 在 AP Role 的下拉框中选择 Root AP 或者 Mesh AP，配置桥接组名。

⑤ 单击 Apply 按钮，应用所有设置。

4.5.5 验证 Mesh 连接状态

配置好 AP 的 Mesh AP 角色后，需要将 Mesh AP 的以太网连接断开，Mesh AP 会通过 Backhual 加入到 Mesh 网络，并出现在控制器的 AP 列表里。

在 WLC 中，通过 Wireless>Access Points>All APs，可以查看 RAP 的 Neighbor Info，验证 Mesh 配置，如图 4-70 所示

All APs > RAP > Neighbor Info　　< Back

Mesh Type	AP Name/Mac	Neighbor Backhaul MAC	Source Backhaul MAC	Slot ID	Neighbor Channel	Source Channel
Child	MAP-1532	20:BB:C0:72:2B:90	0C:D9:96:4D:91:9F	1	149	149
Child	MAP-1042	C0:25:5C:83:97:A0	0C:D9:96:4D:91:9F	1	149	149
Child	MAP-3602	F8:4F:57:84:BA:40	0C:D9:96:4D:91:9F	1	149	149

图 4-70　验证 Mesh 连接状态

还可以在 WLC 中通过命令行的方式验证 Mesh 连接状态：

```
(Cisco Controller) >show mesh ap tree
 ==========================================
||   AP Name [Hop Counter, Link SNR, Bridge Group Name]   ||
 ==========================================
[Sector 1]
----------
RAP[0,0,LAB]
  |-MAP-3602[1,30,LAB]
  |-MAP-1532[1,27,LAB]
  |-MAP-1042[1,28,LAB]
----------------------------------------------------
Number of Mesh APs................................ 4
Number of RAPs....................................... 1
Number of MAPs..................................... 3
----------------------------------------------------
```

4.5.6 设置全局 Mesh 参数

为了使 Mesh 网络更优化运行，需要设定 Mesh 的各种参数，全局参数的设定对每个 AP

都会产生作用，其设置步骤如下所述。

① 导航到 Wireless > Mesh，打开 Mesh 页面，如图 4-71 所示。

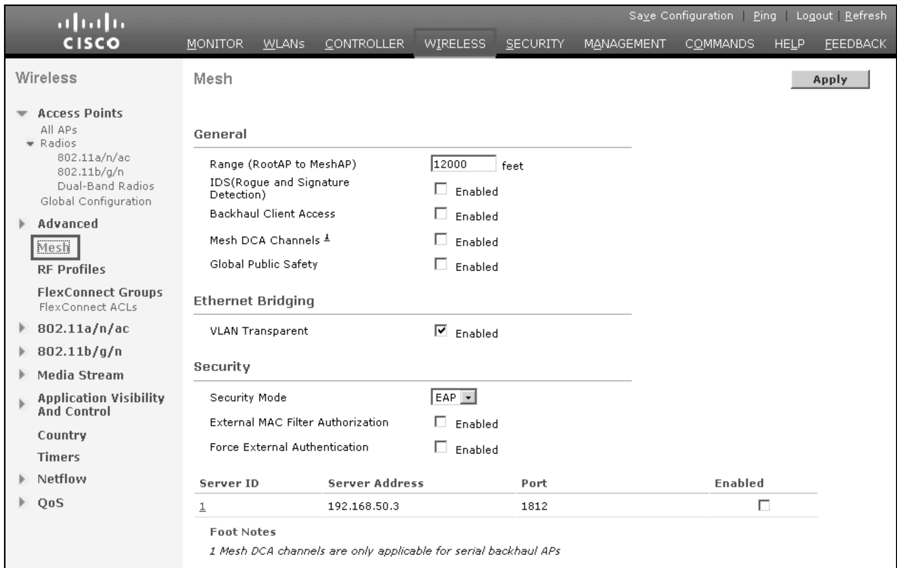


图 4-71　配置 Mesh AP 的全局参数

② 根据需要修改 Mesh 参数。

- Range（Root AP to Mesh AP）：RAP 与 MAP 之间的最佳距离，从 150 ～132 000 feet，仅对室外 AP 生效，设置完成后，所有的室外 Mesh AP 将重启。
- Backhaul Client Access：由于 Mesh 之间使用 IEEE 802.11a 传输数据，如果使能 Backhaul Client Access，则用户可以通过 IEEE 802.11a 关联到 Mesh AP，否则用户只能通过 IEEE 802.11b/g 关联到 Mesh AP。设定这个选项将会重启 AP。
- VLAN Transparent：去使能此选项将允许 Mesh AP 传输 Tagged 的 VLAN 数据，否则只能传输 Access VLAN（Untagged VLAN）的数据，遇到 Tagged 的 VLAN 数据将会自动丢弃。
- Security Mode：EAP 或 PSK 安全模式，如果到外部认证 MAC 地址，则只能选择 EAP 模式。

③ 单击 Apply 按钮使修改生效。

④ 单击 Save Configuration 保存更改。

4.5.7　设置本地 Mesh 参数

对于单个 Mesh AP 参数的设定，其中包含两个部分：天线增益和桥接，其设定步骤如下所述。

① 导航到 Wireless > Access Points > Radios > 802.11a/n，打开 802.11a/n Radios 页面，如图 4-72 所示，在弹出的菜单中选择 Configure。

图 4-72　设置 Mesh AP 的参数

② 在 Antenna 参数中，选择合适的天线增益。选择增益时要同天线的出厂说明相匹配，如图 4-73 所示。

图 4-73　配置 Mesh AP 的天线增益

③ 单击 Apply 按钮使修改生效。

④ 单击 Save Configuration 保存更改。

4.5.8　配置以太网桥及 VLAN 标记

以太网桥可用于点对点及点对多点的网络拓扑中，以太网 VLAN 标记允许特定的应用流量被分割，然后通过桥接进入有线网络或另一个无线 Mesh 网。如今一个典型的应用就是无线

的视频流，每一个无线摄像头通过一段有线连接到 Mesh 拓扑中，这些视频流在逻辑上形成单独的一个网络，如图 4-74 所示。

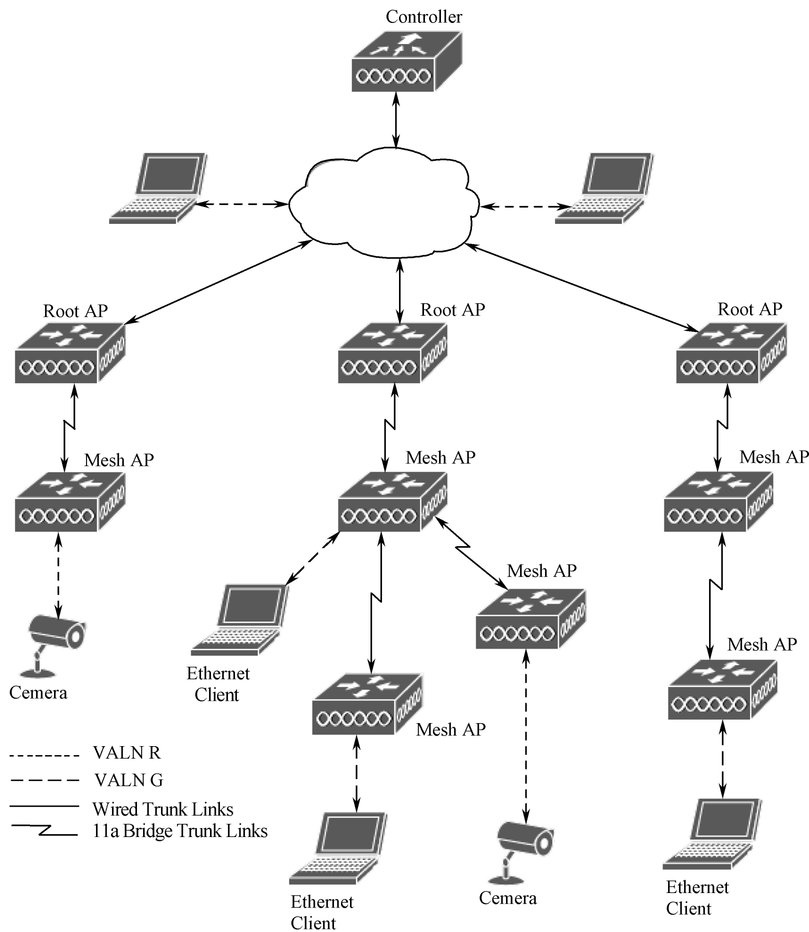


图 4-74　视频流的以太网 VLAN 标记

1．设置 VLAN 标记的注意事项

由于安全的原因，在默认情况下，Mesh AP 的以太网端口是被禁止的，如果需要设置 VLAN 标记，则需要在控制器上手动开启 Mesh AP 的以太网端口，同时需要在全局状态下使能 VLAN 标记功能，只要在全局参数配置时去使能 VLAN transparent 功能即可。

当 VLAN 标记设定后，必须在链路上的每个 Mesh AP 中支持此 VLAN 标记的传输，否则相应的流量见会被丢弃。

VLAN 标记只能在以太网端口上设定，对于 152x 系列的 Mesh AP，可以用 4 个端口中的 3

个端口作为第二（Secondary）以太网端口，分别为 port 0-PoE in、 port 1-PoE out、 port 3- fiber，Port 2 - cable 不能被使用（仅用于同 Cable Modem 相连）。其他只有在 2 个端口的 Mesh AP 中，RAP 上的 port 0-PoE in 可以被用来上连有线的交换机 Trunk 端口，MAP 上的 Port 1-PoE out 可以用来接外部的设备，比如有线的摄像头。用于回传使用的 IEEE 802.11a 用作主（Primary）以太端口，回传路径上使用 Trunk，并将携带所需的 VLAN 标记信息。

在回传的路径上最多支持 16 个 VLAN。

2．配置 VLAN 标记

① 导航到 Wireless > Access Points > All APs 页面，打开所有的 AP 信息。

② 单击所需配置的 AP 以使能以太网桥。

③ 单击 Mesh 标签打开 Mesh 配置详细信息，如图 4-75 所示。

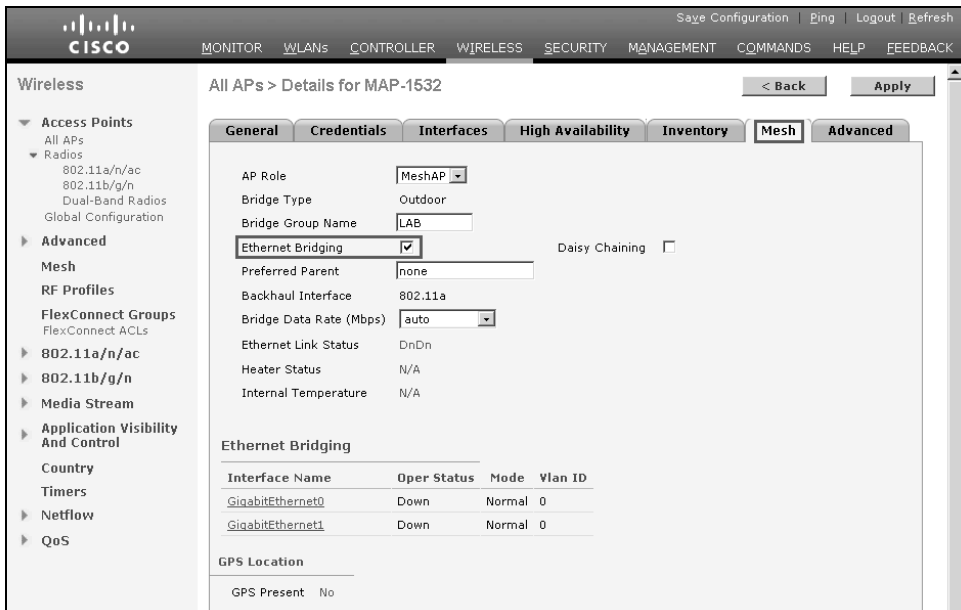


图 4-75　以太网桥接的配置

④ 在 AP Role 的下拉框中选择 Root AP 或 Mesh AP 的角色。

⑤. 如果需要将此 AP 加入到一个桥接组，则在 Bridge Group Name 中输入相应的组名。

⑥ 选中 Ethernet Bridging 的复选框以使能桥接功能。

⑦ 从 Bridge Data Rate 下拉框中选择合适的回传速率，Cisco 建议将此速率设定为 auto，此时 Cisco 设备将会尝试使用最高速率连接。

⑧ 单击 Apply 应用设置。

3. 设定以太网端口为 Access 端口

① 单击 gigabitEthernet1 (port 1-PoE out)。
② 从下拉列表中选择 Access。
③ 选择一个 VLAN ID，其值从 2～4095。
④ 设定以太网端口为 Trunk 端口。
⑤ 单击 gigabitEthernet1 (port 0-PoE in)、gigabitEthernet1(port 1-PoE out)或者 gigabitEthernet1 (port 3- fiber)。
⑥ 从下拉列表中选择 Trunk。
⑦ 输入 Native VLAN 的值，如图 4-76 所示。

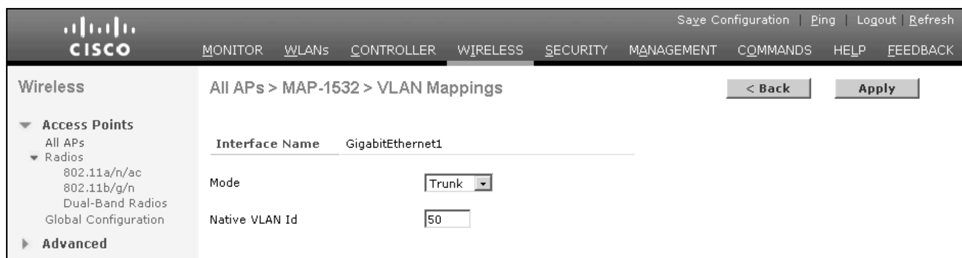


图 4-76　配置 Mesh AP 桥接的 Native VLAN

⑧ 输入 Trunk 的 VLAN ID，如果转发的是没有标记的 VLAN 数据，则 Trunk VLAN ID 的值仍然设为 0（用于 MAP 到 MAP 的连接）；如果转发的是标记的 VLAN 数据，则输入对应的交换机端口上分配的 VLAN 标记（用于 RAP 同交换机的连接）。
⑨ 单击 Apply 按钮应用设置。
⑩ 单击 Save Configuration 保存设置。

4.6　配置 LAP

Cisco 轻量级 AP 是种“无须接触”的设备，几乎不需要人工干预就能够安装并使用它，WLC 能够管理 LAP 的各个方面，其中包括代码映像同步，因此，不需要在 LAP 中预先配置任何信息。

本节介绍安装 LAP 前需要完成的任务。

4.6.1　给 LAP 供电

轻量级 AP 使用直流电，要求的功率最高为 15 W，具体的功率取决于 LAP 的型号和使用的射频类型，例如，当 CiscoAironet 1130AG 以最大发射功率启用 IEEE 802.11a 和 IEEE

802 .11b/g 时，要求的最大功率为 12.2 W。可采取下列方式之给 LAP 供电。

- AC 适配器：如果 LAP 附近有 AC 电源，可通过这种适配器直接将电源与 LAP 连接。
- Power over Ethemet（PoE）：可使用 Cisco 内置电源或 IEEE 802 .3af 方法，通过交换机端口和以太网电缆给 LAP 供电，通过以太网电缆的接脚 I、2 和 3、6 或 4、5 和 7、8 给 LAP 供电。
- 电源注入器：是个小盒子，被插入到交换机端口和 LAP 以太网连接之间，将 AC 适配器直接插入到电源注入器中，通过以太网电缆中的接脚对 4，5 和 7，8 给 LAP 供电，当 LAP 连接的交换机不支持 PoE 时，这种方法很有用。

如果通过以太网电缆供电，由于电缆消耗能量，可能增大 LAP 的功率需求。例如，如果使用 100 m 的电缆，LAP 要求的最大功率可能增加大约 2.5 W，从 12.2 W 增加到 14.7 W。

当使用 PoE 通过交换机接口给 LAP 供电时，与使用这种方式给 Cisco IP 电话供电没有什么不同，有关给交换机配置 PoE 的信息，请参阅其他思科文档。

4.6.2 配置连接 LAP 交换机端口

在将 LAP 连接到交换机端口之前，应确保正确地配置了该端口，AP 要求端口为接入模式而不是中继模式。可以将 LAP 放置到交换模块中任何 VLAN 中，例如，AP 可同当前区域内的其他终端一起位于用户接入 VLAN 中。

通常，最佳的做法是预留一个 VLAN，用于传输 LAP 管理数据流，该 VLAN 包含 LAP 预留的一个 IP 子网。

也可以在 LAP 连接的接入模式端口上启用生成树 PortFast，AP VLAN 将在 LAP 处终止，而不再进一步向外扩展。因此，该 VLAN 不存在无线网络的某个地方形成环路的风险。

可以使用下面的 Catalyst IOS 命令来配置连接 LAP 的交换机端口。

```
!Define the LAP access VLAN
switch（config）# vlan lap-vlan-name
switch（config-vlan）#name lap-vlan-name
Switch（config-vlan）#exit
!Collfigure the LAP switch port
Switch（config）# interface mod/num
Switch（config-it）#switchport
Switch（config-if）#switchport access vlan lap-vlan-num
Switch（config-if）# switchport host
Switch（config-if）#power inline auto
Switch（config-if）#no shutdown
Switch（config-if）#exit
```

4.6.3　LAP 的初始配置

WLC 被正确配置并正常运行后，无须做任何配置就可以将 LAP 加入到网络中，这被称为“零接触”安装。

LAP 只需要以下两条信息就能够启动并与 WLC 通信。

- 一个 IP 地址；
- 一个或多个 WLC 的地址。

可以给 LAP 通电，连接到其控制台端口，并预先配置这些信息，然而，这带来了不必要的管理负担，可以使用网络中的 DHCP 服务器来给 LAP 提供 IP 地址。LAP 需要一个 IP 地址才能同 WLC 交换消息并建立 CAPWAP 隧道，可将这种地址视为管理地址，通常属于交换模块内的管理子网（VLAN），终端用户或无线客户端所需的地址或子网都将通过 CAPWAP 隧道传递给 LAP。

如果 WLC 和 LAP 的管理接口连接的是同一个第二层 VLAN 和 IP 于网，LAP 将能够通过发送子网广播来找到 WLC，位于同一个子网中的 WLC 都将做出应答，让 LAP 能够建立一个 WLC 地址列表。

如果 WLC 和 LAP 位于不同的 IP 子网，当 LAP 收到 DHCP 应答后，将能通过 DHCP 选项 43 的内容来获悉 WLC 的地址，选项 43 的格式随 LAP 型号而异，Cisco 1000 和 1500 系列 LAP 使用用逗号分隔的 WLC 管理接口地址列表。

其他型号的 LAP 使用一个由十六进制位组成的字符串，它表示一个 TLV（类型、长度、值）字段。该字段由如下值组成。

- 类型：一个字节，值为 0xf1；
- 长度：WLC 地址数乘以 4（每个 WLC 的 IP 地址长度字节）；
- 值：WLC 管理接口的 IP 地址。

例如，假设一台基于 IOS 的交换机被用作 DHCP 服务器来向 LAP 提供 IP 地址，则可以使用下面的配置命令：

```
Swich（config）#ip dhcp pool pool-name
Swich（dhcp-config）#network ip-address subnet-mask
Swich（dhcp-collfig）#default-router ip-address
Swich（dhcp-config）#dns-server ip-adress
Swich（dhcp-config）#option 43 {ascii | hex} string
Swich（dhcp-config）#exit
```

假设 LAP 管理子网为 192.168.10.0/24，默认网关为 192.168.10.1，DNS 服务器的地址为 192.168.100.100 ，有 3 个 WLC，LAP 应按下面的顺序与它们联系：192.168.1.10，192 . 168 .1.11 和 192.168 .1.12。

应首先使用如下命令来配置 IOS DHCP 池：

```
Swich（config）#ip dhcp pool lap-pool
Swich（dhcp-config）#network 192.168.10.0 255.255.255.0
Swich（dhcp-collfig）#default-router 192.168.10.1
Swich（dhcp-config）#dns-server 192.168.100.100
```

对于 Cisco 1000 和 1500 系列 LAP，DHCP 选项 43 应类似于下面这样：

```
Swich（dhcp-collfig）#option 43 ascii “192.168.1. 10,192. 168.1.11, 192.168. 1.1 2"
```

而对于其他型号的 LAP，应像下面这样配置 DHCP 选项 43：

```
Swich（ dhcp-config）# option 43 hex oxf1 0cc0a80 10ac0a801 0bc0a80 I0c
```

其中的十六进制字符串从左到右依次如下：

- Oxf1 表示字段类型；
- 0c 表示 WLC 地址列表的字节数，有 3 个 IP 地址，因此总字节数为 12（用十六进制表示为 0C）；
- C0a8010a 是 192.168.1.10 的十六进制表示；
- C0a8010b 是 192.168.1.11 的十六进制表示；
- C0a8010c 是 192.168.1.12 的十六进制表示。

关于 DHCP Option 43 的详细配置参见附录。

CAPWAP 使用 UDP 端口 5246 和端口 5247，应在 LAP 和 WLC 上确保允许通过这些端口，通过使用 WLC Web 界面，可以检查 LAP 的状态，在 Monitor Summary 屏幕中，找到 Access Point Summary 部分，单击 All APs 旁边的 Detail 链接，图 4-77 是个 LAP 状态示例屏幕。如果 Operational Status 栏的值为 REG，则表明 LAP 已启动，建立了到 WLC 的 CAPWAP 隧道，并正常运行。

AP Name	IP Address	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
APb838.612d.4f80	10.5.5.10	AIR-CAP3702E-H-K9	b8:38:61:2d:4f:80	1 d, 00 h 42 m 16 s	Enabled	REG
AP4c00.8207.8a18	10.5.5.11	AIR-CAP3602I-C-K9	4c:00:82:07:8a:18	1 d, 00 h 42 m 01 s	Enabled	REG
AP1	10.5.5.12	AIR-LAP1042N-C-K9	d4:8c:b5:d2:2c:a0	1 d, 00 h 41 m 34 s	Enabled	REG
APc067.afca.4fe9	10.5.5.17	AIR-LAP1042N-C-K9	c0:67:af:ca:4f:e9	1 d, 00 h 26 m 57 s	Enabled	REG
AP4c4e.3546.f372	10.5.5.18	AIR-CAP1532I-H-K9	4c:4e:35:46:f3:72	1 d, 00 h 03 m 07 s	Enabled	REG

图 4-77　显示 LAP 的状态信息

多种型号的 Cisco 接入点可运行在自主或轻量级模式下，使用的模式取决于 AP 运行的 IOS

代码版本，要了解 AP 当前运行在哪种模式下，可连接到控制台端口，并执行命令 show version，如果 Cisco IOS 软件的版本名以后缀 JX 结束，将使用轻量级模式；否则，将在自主模式下运行。在下面的两个示例中，第一个 AP 运行在自主模式下，而第二个 AP 运行在轻量级模式下。

```
ap#show version
Cisco IOS Software, C1130 Softwar(c1130-k9w7-M)，version 12.3(7)JA1 ,RELEASE SOFtWARE(fcl)
Technical Support:http://www.cisco.com/techsupport
Copyright@ 1986-2005 by Cisco systems, inc
Compiled Thu 06-oct-05 09:36 by evmiller

ap#show version
Cisco IOS Software, cl130 Software (c1130-k9w8-M)，version 12.3(7)JX3,RELEASE SOFTWARE (fcl)
Technical Support:http://www.cisco.com/techsupport
Copyright@ 1986-2006 by Cisco systems, Inc Compiled Tue 28-Feb-06 21: 14 by evmiller
```

4.7　控制器冗余及 LAP 的负载均衡

4.7.1　控制器的物理端口及逻辑接口冗余

WLC 可以被配置成采用多个物理端口接入网络，当采用多个物理端口连接到网络时，WLC 的管理接口和动态接口可以被映射到主要和备份端口，在主、备端口之间，不能进行负载均衡，因为同一时刻只能有一个端口被使用。然而，当采用主、备端口时，我们需要配置 2 个 AP 管理接口地址，分别应用到主、备 2 个物理接口，因为 AP 管理接口不支持主、备端口设置。

当启用 LAG（链路聚合）时，流量在多个端口之间是负载均衡的，在启用 LAG 后，在接口配置中没有主、备端口的设置。系统将会自动检测物理接口的连接状态，一旦发现端口连接中断，将会把流量自动切换到活动的端口上。下面我们在讲述主、备端口时都是在没有开启 LAG 的情况下。

如果已经有活动的 WLAN 被映射到相应的接口，为了配置此接口，必须首先禁用 WLAN，禁用 WLAN 的步骤如下所述。

- 导航到 WLAN 菜单，选择相应 WLAN 的 WLAN ID，将 Status 边上的 Enable 复选框去除选择后应用即可禁用相关的 WLAN。
- 导航到 Controller>Interfaces，选择需要更改的 interface，在 Physical Information 中配置备份端口的相关信息后应用，具体如图 4-78 所示。

对除服务接口、虚拟接口及 AP 管理接口之外的其他所有接口设置备份端口，在设置完成后，请为每个备份接口配置一个 AP 管理接口地址。

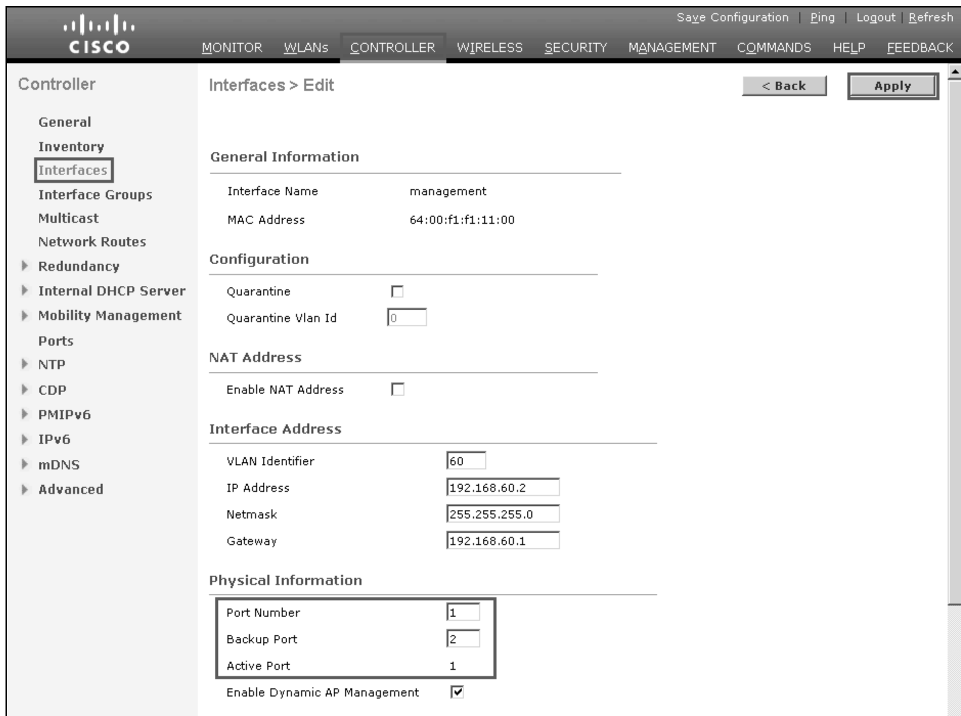


图 4-78　配置控制器的冗余物理端口

通常，我们在配置主、备端口时要考虑网络的最佳连通性，例如，当采用“独背”（One-armed）模式将 WLC 连接到 Catalyst 4500、Catalyst 6500 或 Catalyst 3750 的堆叠时，最好能够将主、备端口连接到交换机不同的模块或堆叠阵列上，以防止模块或堆叠交换机损坏。具体如图 4-79 所示。

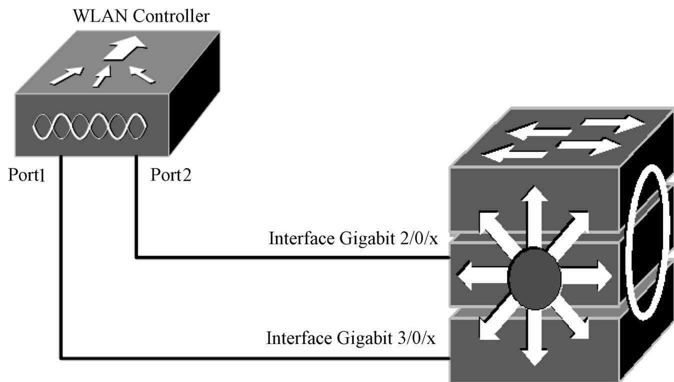


图 4-79　WLC 连接到模块化交换机的推荐方法

设想将 WLC 部署在分发层有冗余交换机（如双核心）的场合，需要将主、备端口分别连接到不同的分发交换机上，如图 4-80 所示。

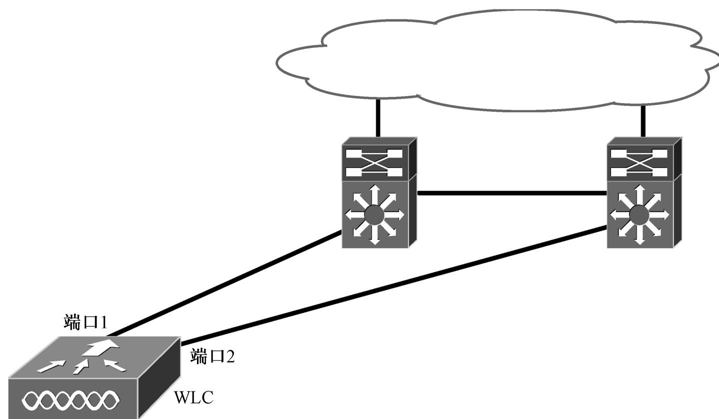


图 4-80　使用冗余端口连接到冗余交换机上

这种分割的上连（Split Uplink）方式在 LAG 模式下并不适用，当 WLC 被配置使用 LAG 模式时，不能将上连线连接到不同的邻居交换机，因为这种方式将会导致 AP 管理接口 IP 的 ARP 查询冲突，然而，可以将上连线分别连接到模块化交换机的不同模块上或堆叠阵列的不同交换机上，并在邻接交换机上配置端口聚合来提供第二层的网络流量负载均衡。

相比主、备端口而言，LAG 模式有如下的一些优点。

① 当采用 LAG 模式时，不需要配置多个 AP-Manager 的地址，因为系统中只有一个逻辑接口。

② 当采用 LAG 模式时，不需要为每个接口配置主、备端口。

③ 当采用 LAG 模式时，单个链路中断时不会用户流量造成影响。

④ 当采用 LAG 模式时，可以在多个链路上实现负载均衡。

但在采用 LAG 模式后，端口镜像及配置多个不打标记的 VLAN 接口都将被禁止。

LAG 模式在 440X 和 5508 系列的控制器中默认是禁用的，而在 WiSM 等集成的控制器模块中默认是开启的。

在 WLC 的 Web 管理界面下开启 LAG 模式，如图 4-81 所示，导航到 Controller>General，将 LAG Mode on Next Reboot 参数改为 Enabled 以实现负载均衡。

4.7.2　LAP 的负载均衡

CAPWAP 协议支持动态冗余及负载均衡，如果在 DHCP Option 43 选项中指定超过一个控制器的 IP 地址，LAP 将会向所有的 WLC 的 IP 地址发送 CAPWAP 的发现请求，在控制器返回的响应中包含了当前已经关联的 AP 数量、能够承受的 AP 总数量及已经连接的用户数。LAP

将尝试加入那些具有最大空闲 AP 的控制器。

图 4-81　配置控制器 LAG 模式

这种动态的负载均衡可以作为一个基本的控制器间的动态负载均衡，一旦 AP 加入了 WLC，将周期性地发送 CAPWAP 的心跳信息给 WLC（默认时间为 30 s），WLC 将采用单播方式进行响应；一旦 AP 丢失一个心跳响应报文，它将以 1 s 的间隔连续发送 5 个心跳报文，如果 5 s 内没有收到任何响应，AP 将自动重新启动并触发新一轮的 WLC 查找过程。

当一个 LAP 关联到 WLC 时，它将会从本地 WLC 的 Mobility Group 获得 Mobility Group 内其他 WLC 的 IP 地址，AP 将会向 Mobility Group 中的每个成员发送查询报文，WLC 返回的响应中包含了 WLC 的类型、容量及当前的 AP 负载。如果同 AP 关联的 WLC 开启了 AP Fallback 功能，AP 将会重新关联到较轻负载的 WLC，这样整个系统就可以支持动态的 WLC 冗余。

这种算法可以实现 Mobility Group 成员间的负载均衡，然而，这可能会产生一些管理及性能上的瓶颈。假设在 DHCP Option 43 种指定了 2 个控制器的 IP 地址，当部署第一个 AP 时，它将会关联到第一个 WLC；当部署第二个 AP 时，它又会关联到第二个 WLC（因为第二个 WLC 的负载较轻），第三个将会加入两个中的任意一个，第四个又会加入第三个加入的另外一个，如此往复。当部署完所有的 AP 时，有一半的 AP 会加入第一个 WLC，另一半加入另一个 WLC，AP 加入控制器时是一个随机状态，用户端在 AP 覆盖范围内移动时，将会不停地在两个 WLC 之间切换漫游，同时这种方式给 LAP 的软件升级及故障诊断都将会带来很大的挑战。

因为负载均衡和控制器冗余产生了不希望出现的这些负面效应，Cisco 提供了一个功能，允许管理员重写 AP 关联的 WLC，静态将 AP 关联到特定的 WLC，这可以通过指定 AP 的主、

次及第三控制器来实现，如图 4-82 所示。在进行这样操作以后，WLC 之间的冗余将会处于一种可控的状态，一旦 AP 指定了主、次及第三控制器，AP 的故障切换将会相当迅速地完成。

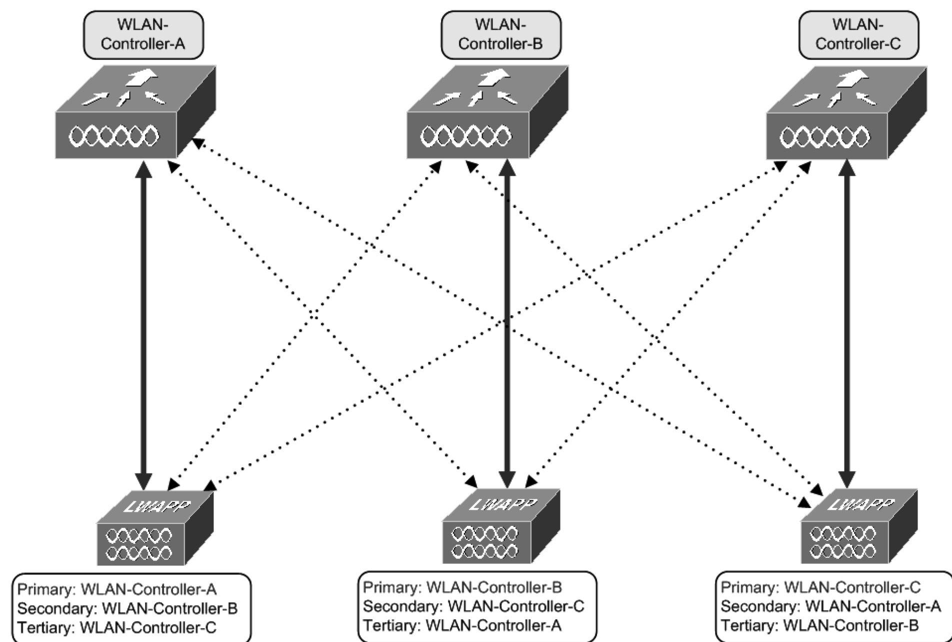


图 4-82 可控的 WLC 之间的负载均衡

当一个 AP 失去同主控制器的联系时，它将会尝试加入次要控制器，如果加入次要控制器失败，将会再次尝试加入第三控制器，如果加入三个控制器都失败，AP 将会根据 CAPWAP 算法加入具有最小负载的 WLC。

WLC 有一个 AP Fallback 参数，配置此参数后，AP 如果由于主控制器的失败失去了与之关联，当主控制器重新联机后，AP 将会重新关联到主控制器。然而当 AP 与主控制器重新关联时，将有一段关联时间（通常为 30 s），在这段时间内，无线客户端可能会失去与网络的连接，如果主 WLC 再次失败，AP 可能会在控制器之间来回摆动，所以大部门网络管理员一般倾向于关闭 AP Fallback 功能，使用计划任务在特定的时间将 AP 转回到主控制器上。

4.7.3 使用 WLC 的 Web 界面配置 AP 的主、备、第三控制器

使用下列步骤，在 Web 管理界面上完成控制器的冗余配置：导航到 Wireless>Access Points>All APs，在 AP 列表中选择需要修改的 AP 并点击其链接，在 AP 的配置窗口中选择 High Availability 选项卡，分别在 Primary、Secondary、Tertiary 文本框中输入控制器的名称及 IP 地址，如果这些控制器在一个 Mobility Group 内，IP 地址可以省略，如图 4-83 所示。

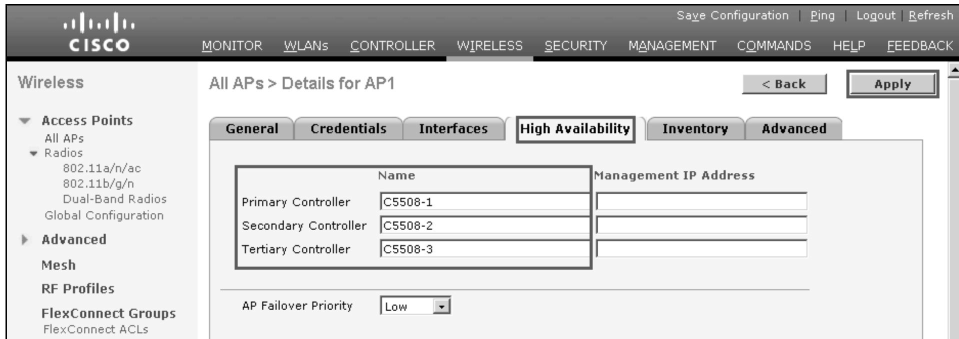


图 4-83　配置 AP 的主、备、第三控制器

AP Failover Priority 表示当某个 AP 由于失去同主 WLC 的关联而寻找同次 WLC 的关联时，如果次 WLC 的关联已满，如果此 AP 的优先级足够高，那么将会替代次 WLC 中低优先级的 AP。

要启用 AP Failover Priority 功能，必须在全局模式下使能此功能，导航到 Wireless>Access Points>All APs>Global Configuration，将“Global AP Failover Priority”参数的属性改为 Enable 并单击 Apply 按钮，如图 4-84 所示。

在此页面中，还可以启用快速心跳模式，以便在发生故障时可以快速切换 WLC。该页面下方还可以设置 Backup-primary 及 Backup-Secondary 控制器，以便当 Primary、Secondary 及 Tertiary 控制器都失效时使用。

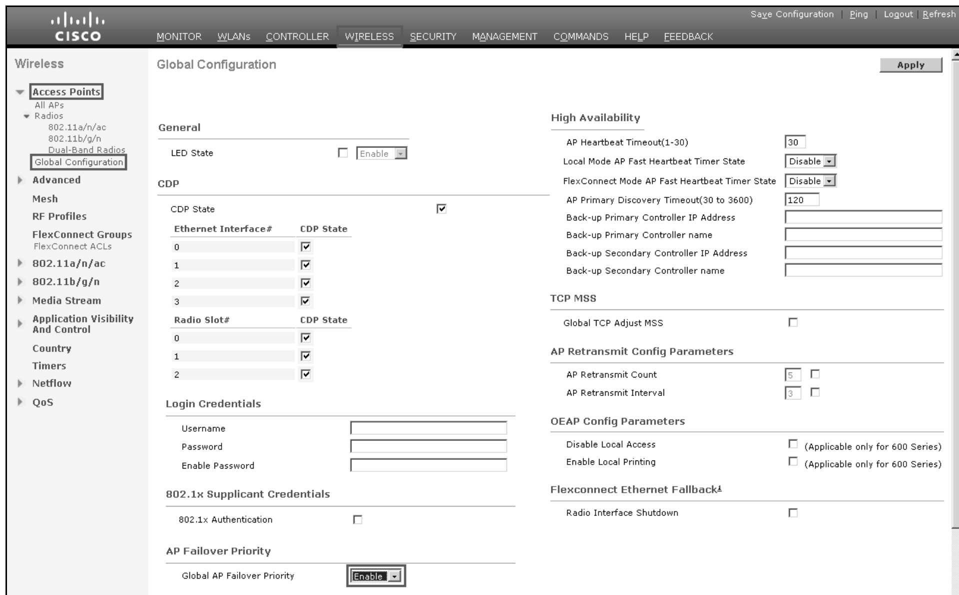


图 4-84　开启 Global AP Failover Priority 功能

4.7.4　使用 WCS 配置 AP 的主、备、第三控制器

在 WLC 的 Web 管理界面中为每个 AP 都指定 Primary、Secondary、Tertiary 控制器是一项相当烦琐的工作，但 WCS 提供了模板用来实现此功能，可以对 AP 进行批量操作，使用下列步骤在 WCS 管理界面上配置控制器的冗余。

首先确保所有的控制器都已经加入了 WCS 中，然后导航到 Configure>AP Configuration Templates>Lightweight AP，在右上角的命令列表中选择 Add Template，单击 GO 提交后为 Template 命名并保存。

在接下来的页面中，选择 AP Parameters 的选项卡，选中 Controllers 边上的复选框，然后从下拉列表中选择合适的 WLC，如图 4-85 所示。当设置完成后，选择 Select APs 的选项卡，选择相关的 AP 后选择 Apply/Schedule 的选项卡，立即应用设置或放入任务计划。

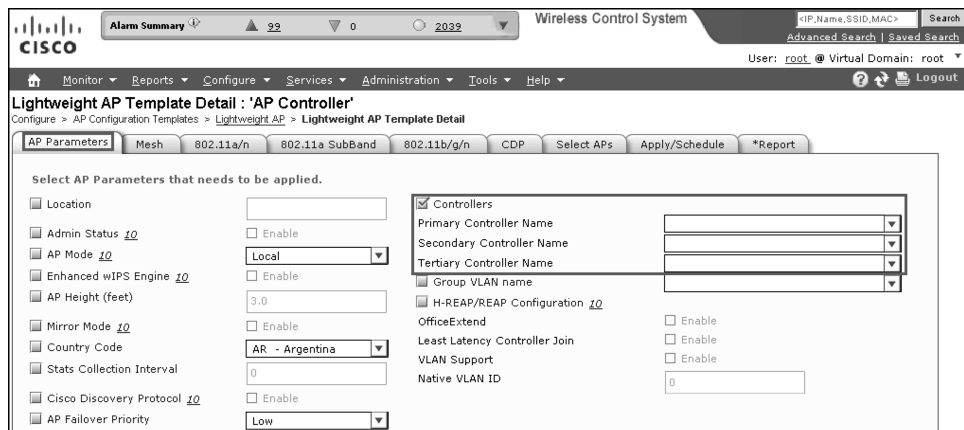


图 4-85　使用 WCS 模板配置 LAP 的主、备、第三控制器

4.7.5　控制器冗余设计

Cisco 统一无线架构提供了多种方式设定控制器的冗余，图 4-86 就是一种典型的 $N+N$ 的冗余设计。

在这种配置方式中，存在 2 个控制器，一些 AP 在将控制器 A 作为主控制器的同时将控制器 B 作为次要控制器，剩下的 AP 将控制器 B 作为主控制器而将控制器 A 作为次要控制器。在这种方式下，需要将 AP 进行分组以便关联到不同的控制器，同时还要尽量减少 WLC 之间的漫游切换。此外，当一个控制器出现故障时，另外一个控制器要能够有足够的授权来承受故障 WLC 上的 AP。

另外一种方式就是 $N+1$ 冗余，如图 4-87 所示。

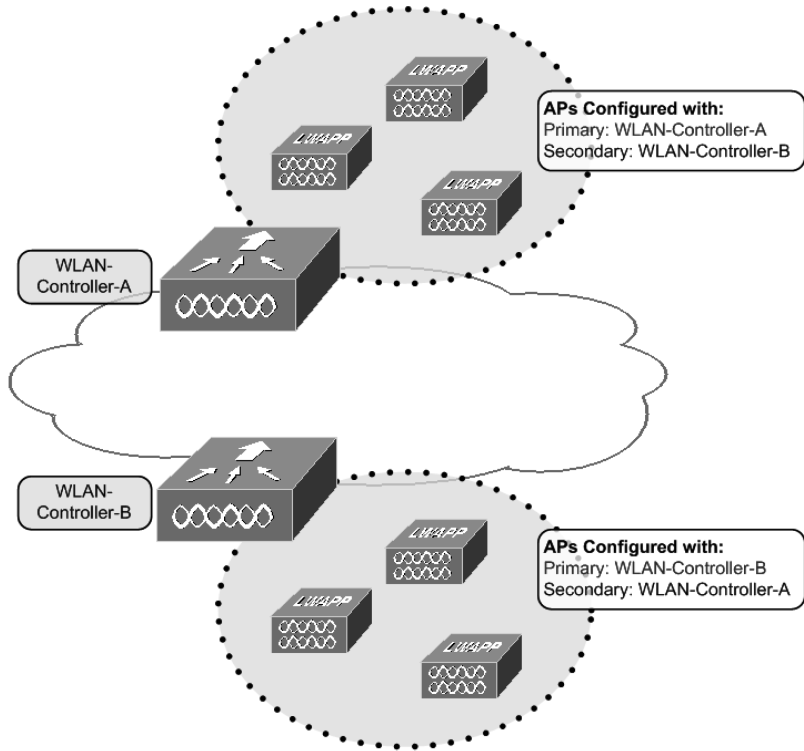


图 4-86 配置控制器的 *N*+*N* 冗余

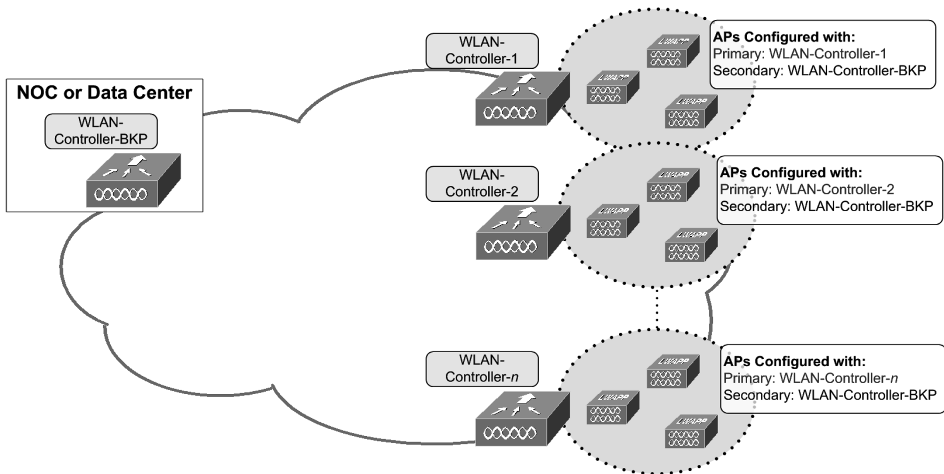


图 4-87 配置控制器的 *N*+1 冗余

在 *N*+1 冗余方式中，冗余的控制器被放在网络运营中心的数据中心，同时作为多个 WLC

的备份。每个 AP 都被配置一个主要控制器，同时将所有的次要控制器都指向同一个备份的 WLC 上，由于两台控制器同时出现故障的概率很小，基本不会产生 AP 无法关联到次要控制器的情况。

最后一种就是 N+N+1 冗余的情况，如图 4-88 所示。

在 N+N+1 这种配置方式中，一些 AP 将控制器 A 最作为主要控制器，将控制器 B 作为次要控制器，剩下的 AP 将控制器 B 作为主要控制器，将控制器 A 作为次要控制器，所有的 AP 都将备份控制器作为第三控制器。一般来说，在这种方式下，主要控制器和次要控制器都放在分发网络中，而备份控制器放置于网络运营中心或数据中心，多个分发地点的 AP 都可以将备份控制器作为第三控制器。

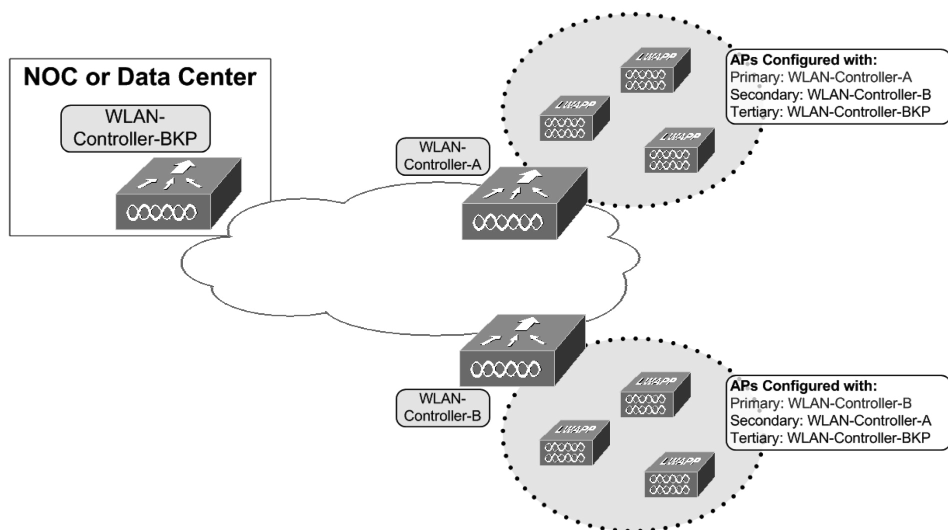


图 4-88　配置控制器的 N+N+1 冗余

4.7.6　快速 AP 故障转移

在早期的 WLC 版本中，LAP 与 WLC 之间采用 LWAPP 协议，一旦 AP 同与之关联的 WLC 失去联系，LAP 启动内部过期时钟，时钟过期时间为 1 s，当时钟超时后，AP 将向配置文件中其他冗余的 WLC 发送注册请求。当 WLC 的映像文件升级到 5.2 版本及更高版本后，LWAPP 协议被 CAPWAP 协议取代，但 CAPWAP 协议中规定 LAP 与 WLC 之间的超时时钟为 3 s，这必然会引起 LAP 的故障切换时间变长。

当一个 WLC 无法提供服务时，与之关联的 LAP 将会寻找下一个可用的 WLC，在此之前，无线用户的无线网络服务可能会中断，为了尽可能使服务不中断，需要减少故障切换的时间。让我们看一下 LAP 在同下一个可用的 WLC 关联之前需要完成哪些动作。

- AP 发送快速心跳间隔：10 s；
- AP 等待快速心跳响应：3 s；
- AP 确认当前 WLC 不可用需要发送 3 次快速心跳：3×3=9 s。

因此，确认当前 WLC 不可用共需时间 10+3+9=22 s。

查找下一个可用 WLC。

- 如果 DNS 服务器不可用引起超时需要 10 s；
- 最小的发现失败延时需要 1 s；
- 同新的 WLC 关联约需要 2 s。

发现新的 WLC 总共需要 13 s。

这样，AP 故障转移到新的可用 WLC 上共需耗时 35 s，在 35 s 后，网络服务才能继续，但对于一些关键应用以及实时应用，35 s 可能会引起连接中断，为了保证网络服务的延续性，需要对以上的时间进行压缩。

有些用户可能需要等待较少的时间就能够中断网络连接，而有些用户可能更愿意等待，为了适应以上两种需求，新版本中提供了以下可调的时间值。

- 心跳时间（Heartbeat）：1～30 s；
- 快速心跳超时：1～10 s；
- AP 重发间隔：2～5 s；
- AP 重发次数：3～8 s。

当使用每个选项的最小值时，心跳时间 1 s，重发间隔 2 s，重传次数 3 次，AP 需要最短 1+2+2×3=9 s 可以发现本地 WLC 故障。

发现下一个 WLC，最短时间为 1+2=3 s，因此，AP 将会在最短 12 s 内取得同下一个可用 WLC 的关联。

由于 WLC 5500 是 4400 的升级产品，在没有采用新版本映像之前，AP 的故障恢复时间明显变长，如表 4-3 所示。

表 4-3 早期版本中各类别控制器心跳时间对比

	5500	WiSM2	2504	7500	440X	210X
心跳时间 / s	10～30	10～30	10～30	10～30	1～30	1～30
快速心跳时间 / s	10～15	10～15	10～15	10～15	1～10	1～10

在最新版本的 WLC 映像中，已经将相应的心跳时间做了一些调整，如表 4-4 所示。

表 4-4 最新版本中各类别控制器心跳时间对比

	5500	WiSM2	2504	7500	440X	210X
心跳时间 / s	1～30	1～30	1～30	10～30	1～30	1～30
快速心跳时间 / s	1～10	1～10	1～10	1～10	1～10	1～10

如果需要在 GUI 界面中配置表 4-4 中的值，请导航到 Wireless>Access Points>Global Configuration，即可以修改相关的参数设置，如图 4-89 所示。

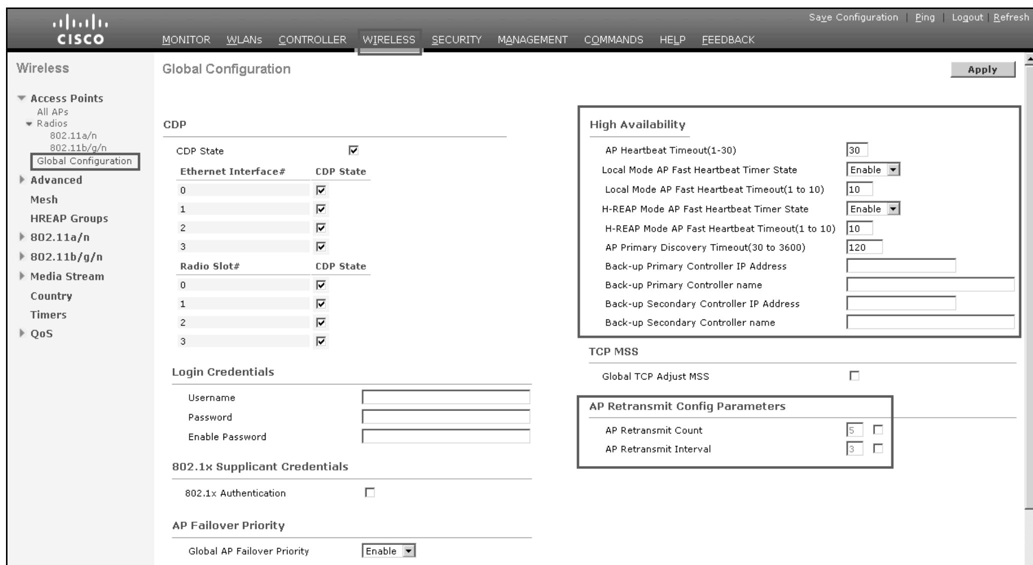


图 4-89　修改 AP 快速故障切换

4.8　管理非法 AP

非法 AP 可以对现有的无线网络造成很大的危害，它可以干扰合法 AP 的正常运行，可以窃取使用明文通信的报文，可以进行 DOS 或中间人攻击，黑客可以用非法 AP 来窃取用户的敏感数据，如用户名和密码，还可以发送一连串的 CTS 报文给 AP，AP 及其他用户接收到报文后，将进行等待操作，这就造成其他合法用户不能访问网络资源，由于这些原因，我们需要阻止非法 AP 接入网络。

因为目前 AP 价格非常便宜，一些员工经常将一些非授权的 AP 接入到有线网络中，这些 AP 可能引发重大的网络安全问题，因为这些 AP 直接位于防火墙以内的内部网络中，其他用户可以不需要认证而直接接入内部网，从而造成内部敏感信息被窃取。

控制器将会指导 LAP 周期性地探测周边是否存在非法的 AP 及连接非法 AP 的用户，如果控制器发现一个非法 AP，它将采用非法定位发现协议（Rogue Location Discovery Protocol，RLDP）来确认非法 AP 是否接入内部网络。可以在控制器上配置所有 AP 或者仅部分只监听 AP 使用 RLDP 协议来侦听非法 AP 信息，后一种模式可以很方便地在非常拥挤的 RF 信道空间中监控自主 AP，这种监控对正常的数据传输没有任何干扰，如果在所有的 AP 上开启 RLDP 功能，如果一个非法 AP 周围既有普通监控 AP 也有只监控 AP，那么控制器一般只选择仅监控

AP 进行操作。如果 RLDP 断定非法 AP 在内部网络中，管理员可以选择自动或者手动阻止非法 AP。

运行 5.0 版本以后的控制器改进了对非法 AP 进行分类和报告的功能，这主要通过非法状态与用户自定义的分类规则实现。在早期版本中，控制器将根据 MAC 地址或 BSSID 列出所有非法 AP 的地址。在新版本中，我们可以创建一些规则让控制器自动将非法 AP 分类为友好的（Friendly）、有恶意的（Malicious）或未分类的（Unclassified）。默认情况下，没有任何分类规则被应用，所有未知的非法 AP 都将被分类为没有归类的，当创建一个规则后，配置触发的条件，应用此规则，那么未分类的 AP 将会被归类，当创建任何一个分类规则后，此规则都将被应用到所有的非法 AP，包括 Friendly，Malicious 以及 Unclassified。

当一个控制器从其管理的 LAP 处收到一个非法 AP 的报告时，它将采取如下的动作：

① 控制器在信任的 MAC 地址列表中查询此非法 AP 的 MAC 地址，如果找到，则将此 AP 划归为友好的（Friendly）。

② 如果此非法 AP 的 MAC 地址不在信任列表中，控制器将开始应用非法 AP 分类规则。

③ 如果此非法 AP 已经被分类为有恶意的（Malicious）、警告的（Alert）、友好的（Friendly）、内部的（Internal）或外部的（External），控制器将不会自动对其进行分类。

④ 控制器将会根据优先级应用所有的分类规则，如果非法 AP 符合规则，控制器将会根据规则分类此非法 AP。

⑤ 如果非法 AP 不能匹配任何已经设定的规则，控制器将会标识此非法 AP 为未分类的。

⑥ 控制器对所有检测出的非法 AP 应用以上几条规则。

⑦ 如果 RLDP 检测出非法 AP 在本地网络上，控制器将会自动认为此非法 AP 是有破坏性的并将它标识为有恶意的 AP，即使没有应用任何规则，也可以手动对此 AP 进行阻止，当然可以通过规则自动对这类非法 AP 进行阻止。如果非法 AP 不在本地网络上，控制器将会把此非法 AP 标记为警告的（Alert），此时可以通过人工方式手动阻止此 AP。

⑧ 根据需要，可以手动将任何一个非法 AP 在不同的分类组之间进行移动，以改变其非法状态。

非法 AP 的分类如表 4-5 所示。

表 4-5 非法 AP 的分类

基于规则的分类	非 法 状 态
友好的（Friendly）	内部的（Internal）——如果未知的 AP 在本网内且对其他无线没有任何危害，可以手工将此 AP 配置为友好的、内部 AP，例如，实验室内部的 AP 外部的（External）——如果未知的 AP 不在本地网络且对其他无线没有任何危害，可以手工将此 AP 配置为友好的、外部 AP，例如，邻居咔吧的 AP 警告的（Alert）——如果未知的 AP 不在邻居列表或不在用户自定义的友好 MAC 地址列表中，此 AP 将会被移到警告状态

续表

基于规则的分类	非 法 状 态
有恶意的（Malicious）	警告的（Alert）——如果未知的 AP 不在邻居列表或不在用户自定义的友好 MAC 地址列表中，此 AP 将会被移到警告状态 有威胁的（Threat）——未知的 AP 在本地网络上，同时对本地网络安全有一定的威胁 阻止的（Contained）——未知的 AP 被阻止了 有待阻止的（Contained Pending）——未知的 AP 已经被标记为阻止的，但由于有限的资源，还没有触发相关动作
未分类的（Unclassified）	未定的（Pending）——在第一次检测中，未知的 AP 将会处于未定状态 3 min，在此期间，控制器检测此未知 AP 是否为一个邻居 AP 有威胁的（Threat）——未知的 AP 在本地网络上，同时对本地网络安全有一定的威胁 阻止的（Contained）——未知的 AP 被阻止了 有待阻止的（Contained Pending）——未知的 AP 已经被标记为阻止的，但由于有限的资源，还没有触发相关动作

前面讲到，控制器可以根据定义好的规则自动改变未知 AP 的分类及非法状态，也可以手工将未知 AP 在不同的分类及非法状态间切换，表 4-6 显示了允许的几种转换状态。

表 4-6　允许的分类及非法状态转换

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

如果非法状态为被阻止的（Contained），首先需要解除阻止，然后再更改分类；如果需要将一个非法 AP 从恶意状态转换成未分类状态，则需要首先删除此 AP，然后让控制器重新对它进行归类。

4.8.1　配置 RLDP

① 导航到 Security > Wireless Protection Policies > Rogue Policies > General，打开非法 AP 策略页，从 Rogue Location Discovery Protocol 下拉列表中选择如下几种状态，如图 4-90 所示。

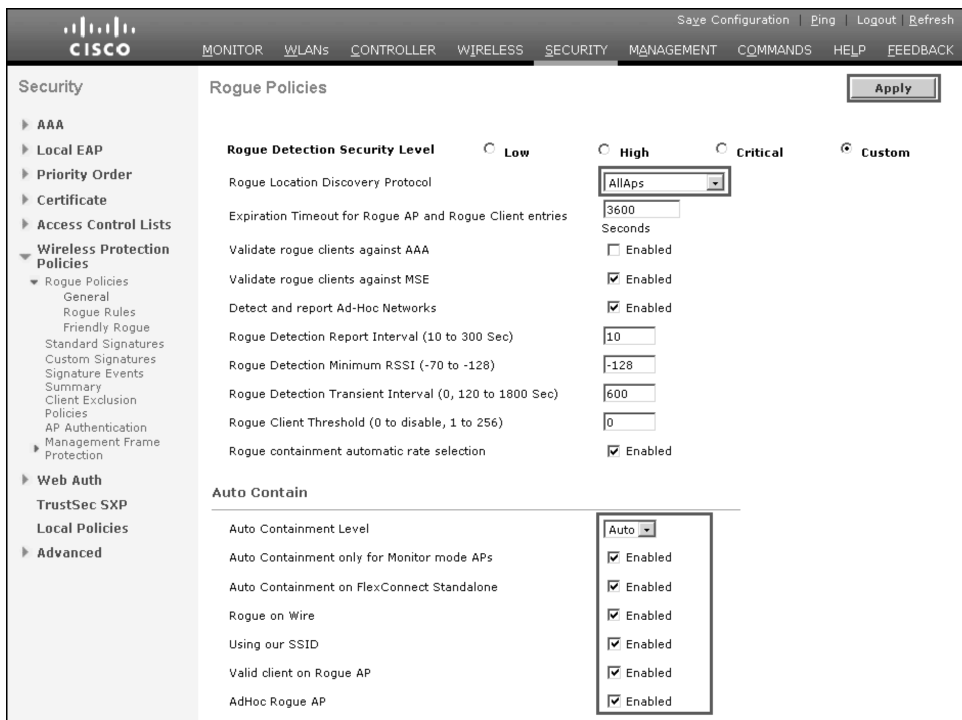


图 4-90 在控制器上配置 RLDP

- Disabled——在所有的 AP 上关闭 RLDP 功能，这是默认的配置。
- All Aps——在所有的 AP 上打开 RLDP 功能。
- Monitor Mode Aps——只在那些仅监控模式的 AP 上启用 RLDP 功能。

② 在 Expiration Timeout for Rogue AP and Rogue Client entries 中设定相应的过期时间，从 240～3 600 s，当设定时间过后，非法 AP 和连接非法 AP 的客户端将会自动从列表中移除，当且仅当非法 AP 的状态为警告的或者有威胁的才能够移除。

③ 如果需要，可以在本地 AAA 服务器上验证连接非法 AP 的客户端是否为合法客户，默认是不选中此项功能。

④ 根据需要，还可以选中 Detect and Report Ad-Hoc Networks 的复选框，以允许对非法 Ad-hoc AP 进行检测和报告。

⑤ 如果需要控制器自动阻止非法的设备，选中 Auto Contain 中包含的复选框，否则将其留在不选中的默认状态。

⑥ 当选中这些复选框时，将会出现如下的警告："使用这些功能可能要承担法律后果，是否继续？" 因为 2.4 GHz 和 5 GHz 的 ISM 频段是不需要任何授权公众就可以直接使用的，阻止其他单位的网络可能会引发法律纠纷。

- Rogue on Wire——自动阻止本地有线网络上的非法 AP。

- Using Our SSID——自动阻止使用本地 SSID 的网络，如果不选中，仅发送一个告警信息。
- Valid Client on Rogue AP——自动阻止那些合法用户连接的非法 AP。
- AdHoc Rogue AP——自动阻止 adhoc 网络。

4.8.2　定义非法 AP 的分类规则

① 导航到 Security > Wireless Protection Policies > Rogue Policies > Rogue Rules，添加分类规则，分类类型中包含 Friendly 和 Malicious，选择 Friendly 或 Malicious，并取名后单击 Add 按钮，如图 4-91 所示。

图 4-91　AP 分类规则

③ 点击所创建规则的 Rule Name 将会出现规则列表，从列表中选择一条进行编辑，如图 4-92 所示。

图 4-92　编辑非法 AP 分类规则

③ 在 Type 下拉列表中选择 Friendly 或 Malicious，Match Operation 选择 Match All 或 Match Any。

- Match All——指需要同时匹配所有的规则。
- Match Any——指匹配规则中的任意一条即可。

④ 选中 Enable Rule 的复选框，以使能此规则，最后选择匹配的条件。

- SSID——非法 AP 必须满足用户指定的 SSID。
- RSSI——非法 AP 必须满足指定的接收功率大小（Received Signal Strength Indication，RSSI），如果超过此功率强度，则被标记为 Malicious。
- Duration——非法 AP 的生存期必须满足指定的时间大小。
- Client Count——同非法 AP 关联的用户必须满足指定的数量。
- No Encryption——非法 AP 没有采用任何加密措施，也就是采用开放式认证的 AP。
- Managed SSID——非法 AP 使用的 SSID 是控制器已知的 SSID

⑤ 添加完毕后，上移或者下移规则可在多条规则之间设定优先级。

4.8.3 查看非法 AP

① 导航到 Monitor > Rogues 即可查看非法 AP 的分类列表，选择任一个分类，将列出此分类中所有的非法 AP，如图 4-93 所示。

Malicious Rogue APs　　Entries 1 - 7 of 7

Remove
Contain
Move to Alert

MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status
00:11:92:5e:84:c0	ECNU	1	1	0	Alert
00:11:92:6e:a9:40	ECNU	6	3	0	Alert
24:de:c6:a8:de:c0	ECNU	11	2	0	Alert
d8:c7:c8:e8:b9:b0	ECNU	11	3	0	Alert
d8:c7:c8:e8:b9:b8	ECNU	149	4	1	Alert
d8:c7:c8:e8:c2:a0	ECNU	6	3	0	Alert
d8:c7:c8:e8:c2:a8	ECNU	157	3	0	Alert

图 4-93　查看非法 AP 列表

④ 选择 MAC 地址，即可得到非法 AP 的详细信息，如图 4-94 所示。

此页包含了非法 AP 的 MAC 地址、非法设备的类别、是否在有线网络上、第一次发现的时间，以及最近一次发现的时间和最新状态。

- Class Type——指明了非法 AP 目前所处的类别。
- Friendly——一个未知的 AP，同用户定义的 Friendly 列表相匹配；一个已知的同时被

用户确认的 AP。Friendly 分类的 AP 不能被阻止。

- Malicious——一个未知的 AP，同用户定义的 Malicious 列表相匹配；是由用户手工从 Friendly 或未分类的类别中移过来的。一旦一个 AP 被标记为 Malicious，以后不能再次对它应用规则，也不能将之移动到其他的分组类别中。如果希望将一个 Malicious 的 AP 移动到未分类的类别中，必须首先删除此 AP，然后让控制器再次发现此 AP 并重新归类。
- Unclassified——一个未知的 AP，不能匹配用户定义的任何规则；一个未分类的 AP 可以直接被阻止，根据用户定义的规则，它可以被自动移动到 Friendly 或者 Malicious 的分类中，当然用户也可自行指定相应类别。

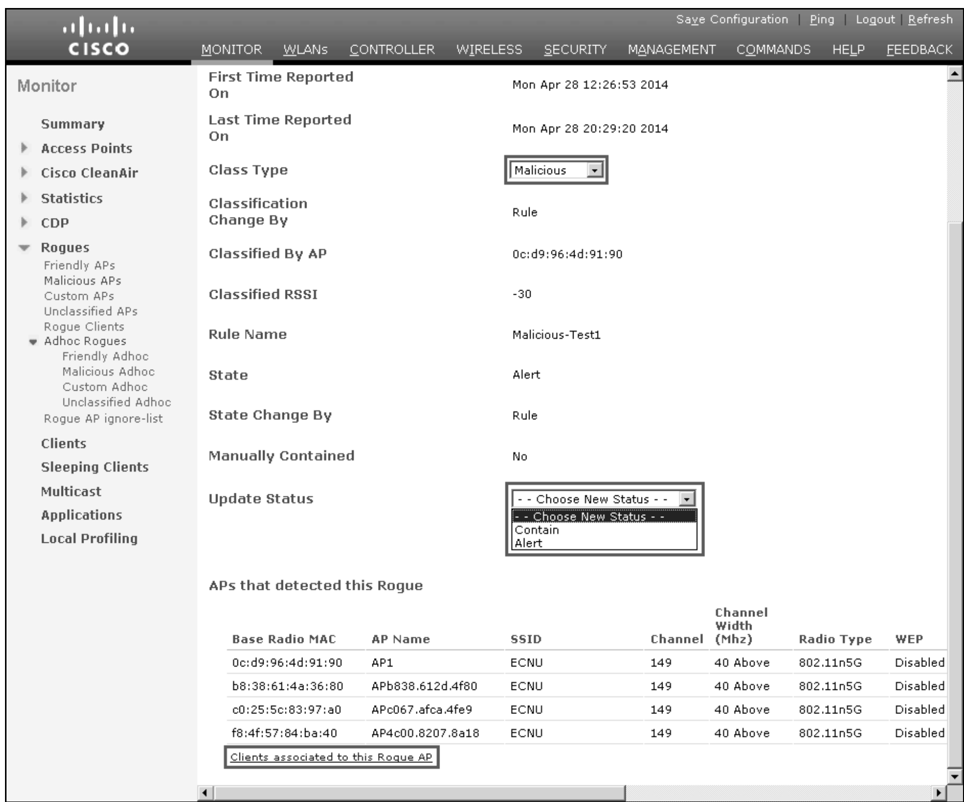


图 4-94　查看非法 AP 详细信息及手动状态更新

③ 从 Update Status 的下拉列表中可以选择如下的动作：

- Internal——控制器信任此非法 AP，仅当分类形式为 Friendly 时才有效。
- External——控制器确认可此非法 AP 的存在，仅当分类形式为 Friendly 时才有效。
- Contain——控制器阻止此非法 AP 的运行，它将不会影响授权用户，仅当分类形式为 Malicious 或 Unclassified 才有效。

- Alert——控制器将立即向系统管理员发送一个告警信息，让管理员采取进一步行动，仅当分类形式为 Malicious 或 Unclassified 才有效。

④ 页面下方还显示了同此非法 AP 关联的客户端的链接，管理员可以进一步查看详细信息和设置状态，设置完成后点击右上角 Apply 应用此设置。

4.9 总结

本章主要介绍了 WLC 的基本配置，下面将统一无线网络中 LAP 和 WLC 的功能做一个总结，如表 4-7 所示。表 4-8 列举了 WLC 各接口的功能。

表 4-7 split-MAC 架构对 AP 功能的划分

功　　能	LAP	WLC
传输和接收 IEEE 802.11 帧	Y	N
帧缓存和 MAC 管理	Y	N
IEEE 802.11 加密	Y	N
RF 管理	N	Y
管理关联和漫游	N	Y
认证客户端	N	Y
管理安全策略	N	Y
处理服务质量	N	Y

表 4-8 WLC 的接口及其功能

接 口 类 型	功　　能	IP 地址
管理接口	带内管理、Web 会话、AAA 服务器	静态 IP 地址，来自一个管理子网
AP 管理接口	CAPWAP 隧道的端点地址	静态 IP 地址，来自一个管理子网
虚拟接口	用于 DHCP 中继的逻辑接口	伪造但唯一的 IP 地址，可能存在于网络的其他地方，通常使用 1.1.1.1
服务端口	在网络中断期间用于带外管理	静态 IP 地址，用于一个特殊的带外子网
集散系统接口	将 WLC 连接到交换型网络，通常是为无线客户端 VLAN 传输数据的中继链路	N/A
动态接口	通过 CAPWAP 隧道将 VLAN 扩展到 LAP	静态的 IP 地址将通过 CAPWAP 隧道扩展到无线客户端的 VLAN

第5章 >>>



认证服务

本章要点

- RADIUS 认证服务创建
- 其他认证方式
- 创建 Guest 账户

Cisco 的无线控制器支持的认证服务方式包括 RADIUS 认证、LDAP 认证和本地认证，如果使用 ACS 作为认证服务器，将会支持更多其他的认证方式。

5.1 RADIUS 认证服务创建

RADIUS 认证必须基于 RADIUS 认证服务器，RADIUS 认证服务器可以采用 Cisco 的 ACS 服务器，也可以采用任何其他标准的 RADIUS 认证服务器，例如，在 Windows 2003 服务器版本中自带的 IAS（Internet Authentication Server），下面将以 Cisco 的 ACS 为例，讲述 RADIUS 认证服务创建的方式。

5.1.1 安装 ACS 服务器并配置

ACS 5.x 预装在 Cisco 基于 Linux 的 ADE-OS（Application Deployment Engine OS）内，可以将该 Linux 安装在物理服务器或者虚拟机上，通过简单的初始化配置和添加授权即可使用。

按照步骤安装 ACS 服务器后， 在客户端浏览器内输入 https://192.168.50.3/acsadmin 访问 ACS 的管理界面。默认登陆用户名为 acsadmin，密码为 default，登陆后会提示更改密码，然后安装授权文件，成功后会出现 5-1 所示的窗口。

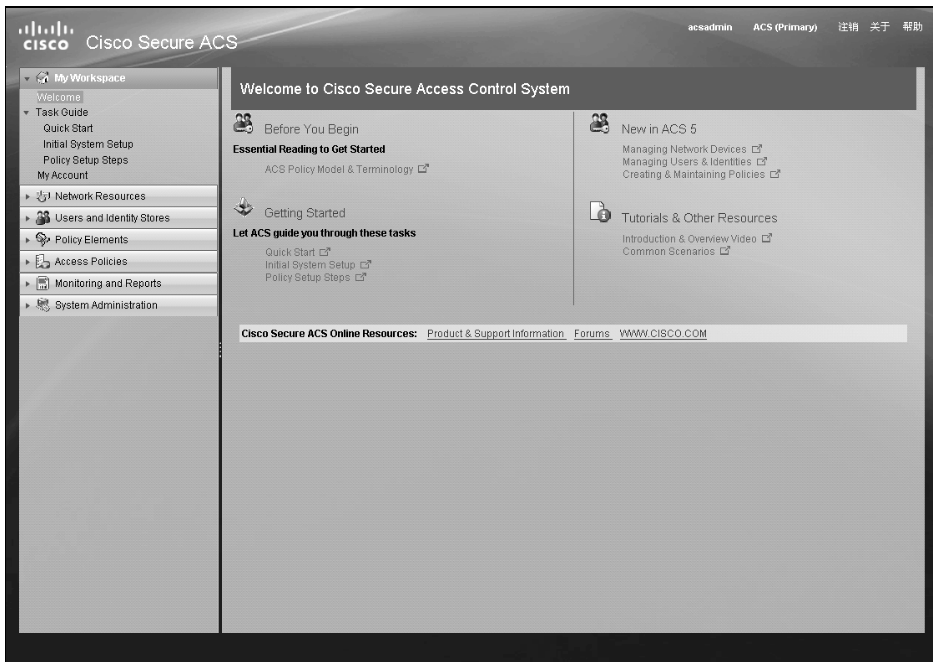


图 5-1 ACS 管理界面首页

ACS 5.x 使用基于规则的策略模型，比 ACS 3.x/4.x 的基于组的策略模型提供了更加灵活的访问控制，其策略模型中的规则以 IF *condition* Then *result* 的形式存在，能限制用户在何种情况下可以访问网络或者当满足特定条件时被赋予一定的权限。配置 ACS 5.x 分为配置网络资源、配置用户、定义策略元素和配置访问服务 4 个步骤。

1．配置网络资源

本例中配置网络资源即是将 WLC 配置为 ACS 的客户端。在 ACS 5.x 中设备分组可以作为规则的条件，还能降低管理复杂度，所以本例中首先配置设备位置组和类型组。选择 Network Resources>Network Device Groups>Location，单击 Create 按钮，创建设备位置组，如图 5-2 所示。

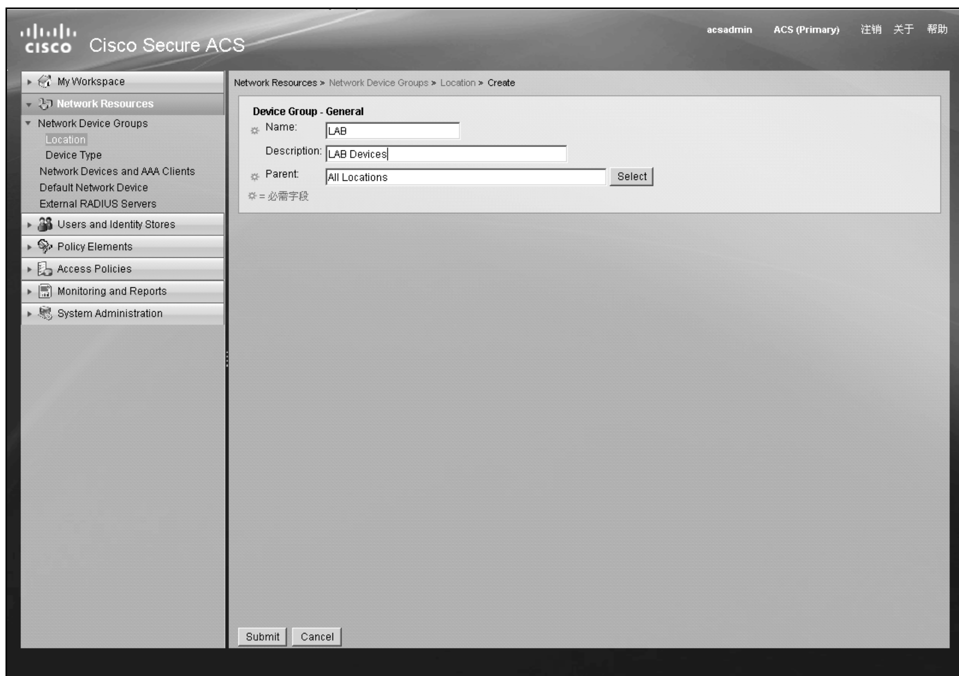


图 5-2　创建网络设备位置组

同样地，点击 Device Type 配置网络设备类型组，如图 5-3 所示。

然后在 Network Resource>Network Device and AAA Clients 页面单击 Create 按钮，为 WLC 选择位置组和类型组，配置其名称、IP 地址（WLC 的 Management 地址）以及 WLC 与 ACS 之间的共享密钥后，单击 Submit 按钮，如图 5-4 所示。

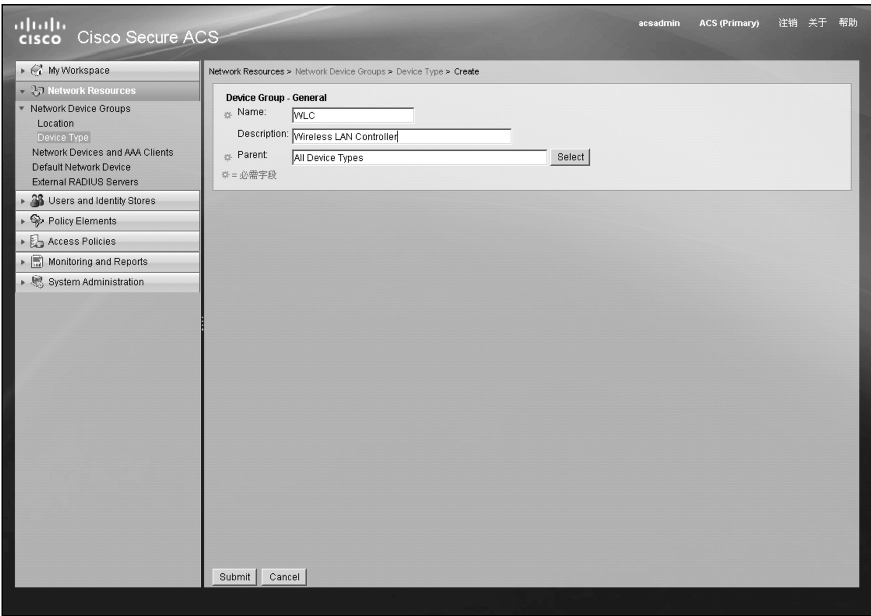


图 5-3　创建网络设备类型组

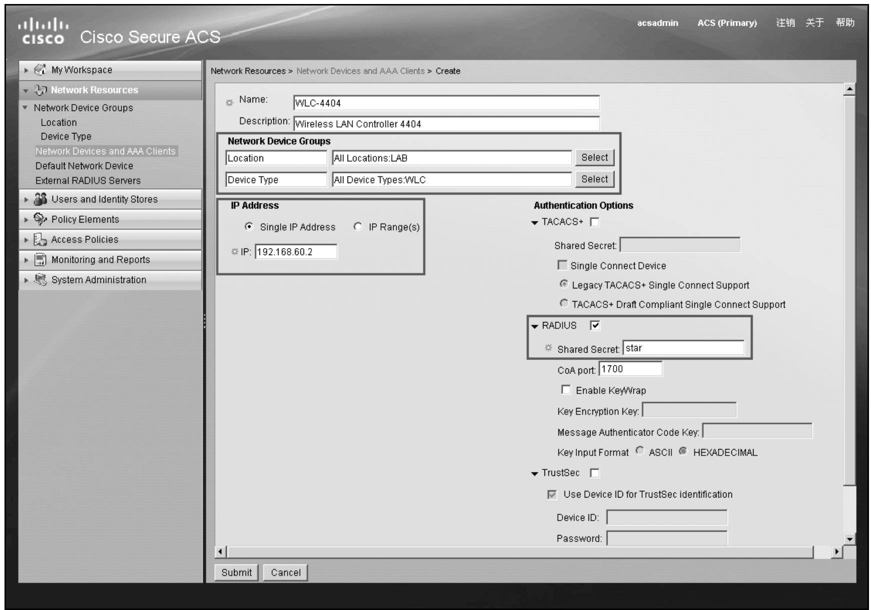


图 5-4　添加 AAA 客户端

2．配置用户

和设备分组一样，通常将用户按照一定类别分组。选择 Users and Identity Stores>Identity

Groups，单击 Create 按钮，输入用户组名称和描述，单击 Submit，如图 5-5 所示。

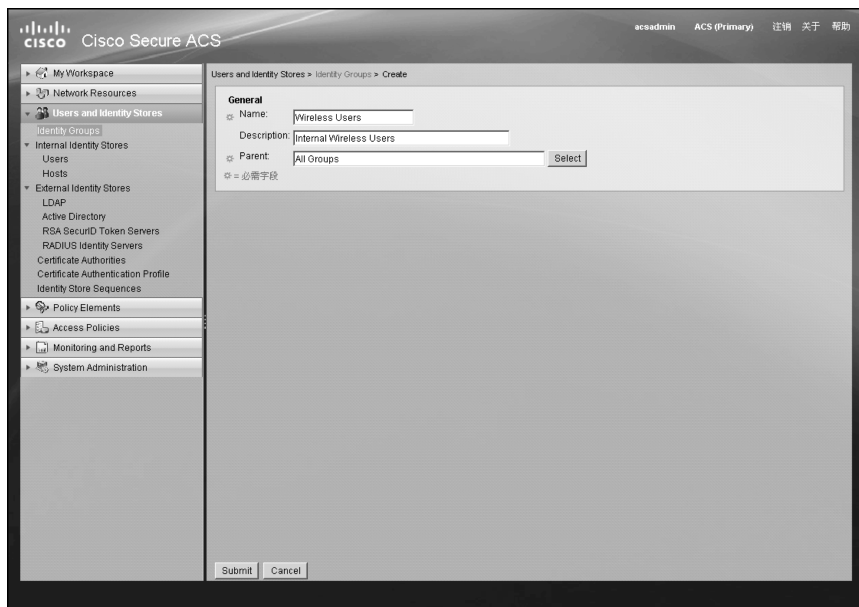


图 5-5　创建用户组

然后添加用户，选择 Users and Identity Stores>Internal Identity Stores>Users，单击 Create 按钮，输入用户名、密码并选择分组后，单击 Submit 按钮，如图 5-6 所示。

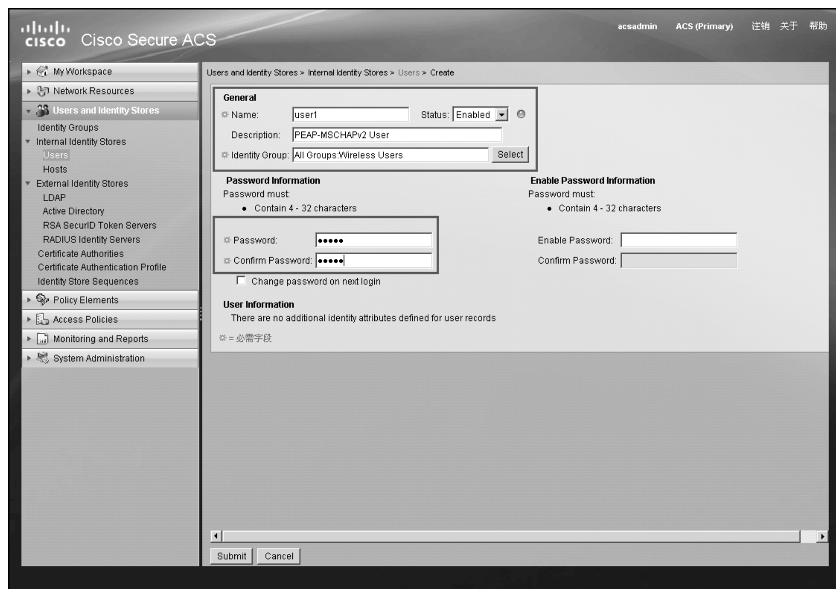


图 5-6　添加用户

3．定义策略元素

ACS 5.x 采用基于规则的授权策略，规则可以同时匹配身份信息、时间、地点、访问类型、终端地址等多种动态条件，还可以自定义授权结果，从而实现灵活的访问控制。在制定规则前，需要配置策略元素，其中包括了条件和授权的定义。在本例中，只需要通过用户信息验证的 user1 就能够访问网络，选择 Policy Elements>Authorization and Permissions>Network Access>Authorization Profile，查看 PermitAccess 授权已经配置，如图 5-7 所示。

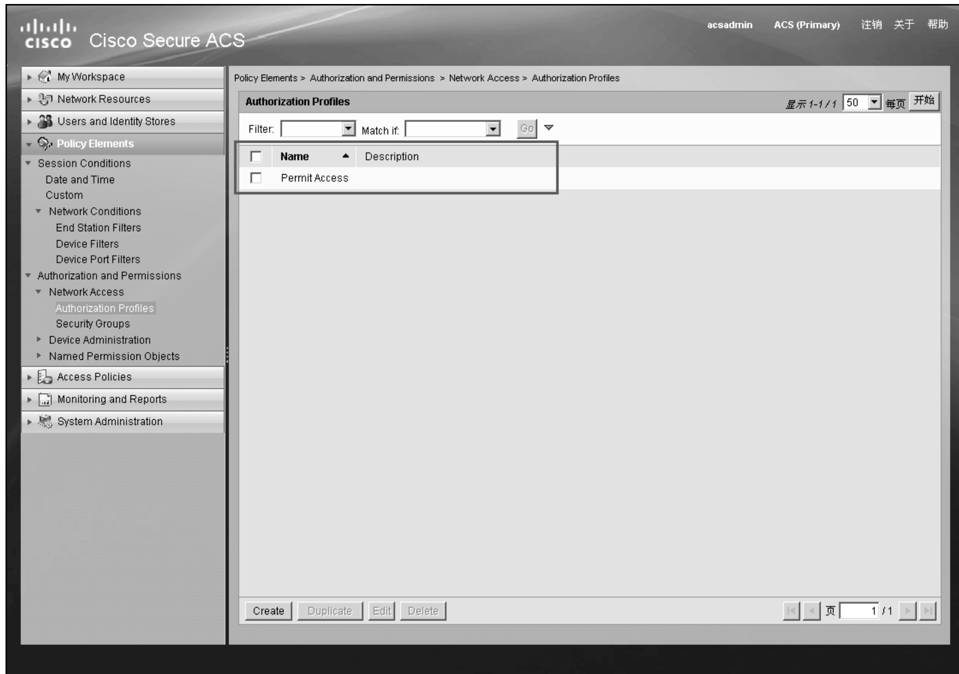


图 5-7　默认配置的 PermitAccess 授权

4．配置访问服务

选择 Access Policies>Access Services>Service Selection Rules，可以选择 ACS 服务器对服务请求的响应方式，选择 Single result selection 表示 ACS 对所有请求执行同一个访问服务内定义的响应；选择 Rule based result selection 表示 ACS 可以基于自定义条件执行不同的访问服务。本例中，选择 Default Network Access 来响应所有的 RADIUS 请求，然后单击 Save Changes 按钮，如图 5-8 所示。

访问服务的配置包括允许使用的认证协议、身份库和授权。选择 Access Policies>Access Services>Default Network Access>Edit:”Default Network Access”，可以配置认证中使用的协议，如图 5-9 所示。

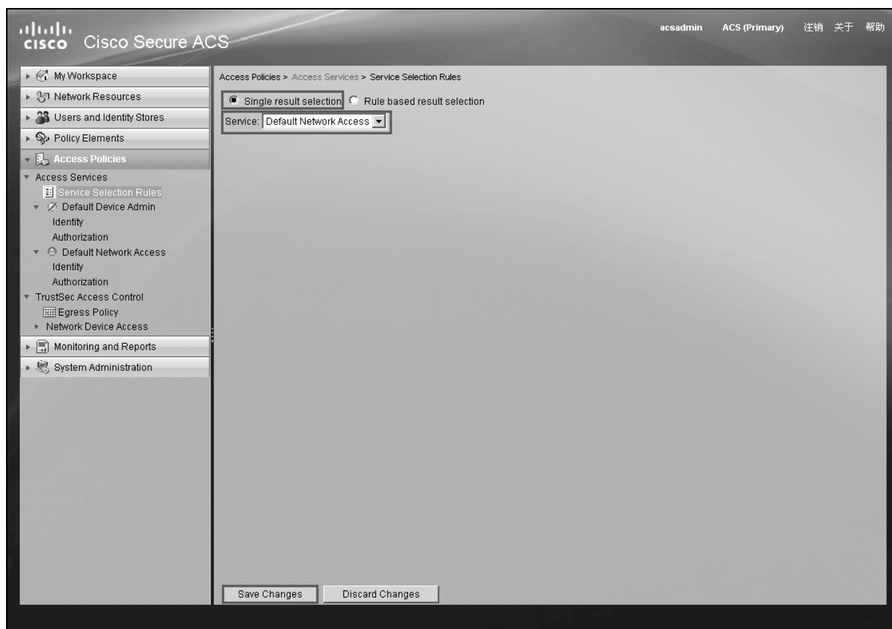


图 5-8　选择请求响应方式

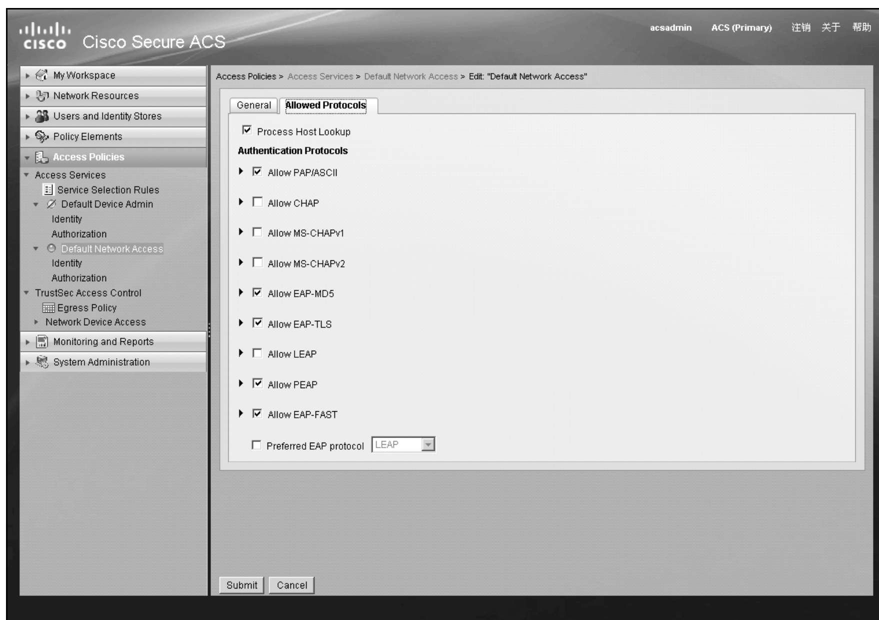


图 5-9　配置认证协议

在身份库的配置中，可以选择使用单一身份库和基于规则的身份库。当选择基于规则的身份库时，能根据不同的条件选择使用不同的身份库，或者根据条件执行 DenyAccess 并发送

Access Reject 的 RADIUS 响应。本例中仅使用 ACS 内部身份库验证 user1，选择 Identity，验证 Identity Source 选择了 ACS 内部身份库，如图 5-10 所示。

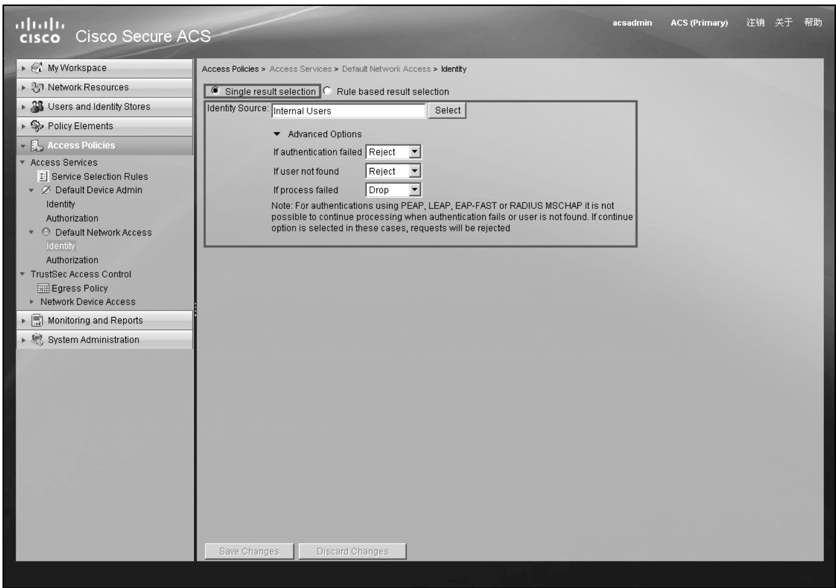


图 5-10　策略中的本地用户

选择 Authorization，单击右下角 Customize 按钮，会弹出对话框，在此界面可以自定义认证规则的条件和结果，然后单击 OK 按钮，如图 5-11 所示。

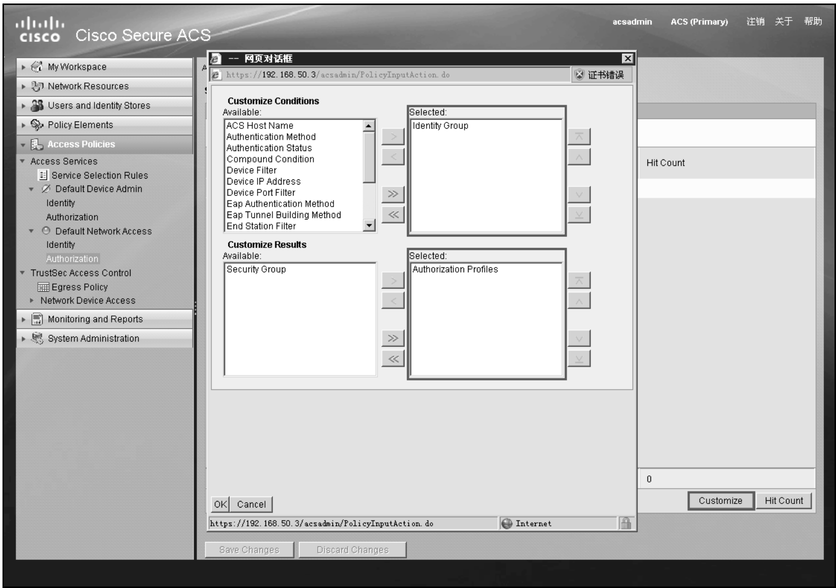


图 5-11　自定义规则的条件与结果

完成规则形式的制定后，可以单击 Create 按钮创建策略中的规则，如图 5-12 所示。

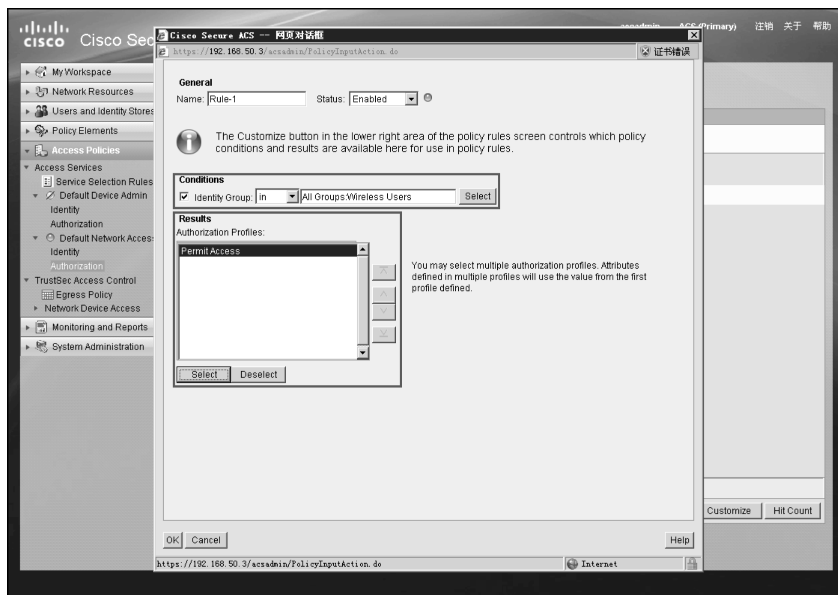


图 5-12　创建策略中的规则

创建完成后，修改默认规则为 Deny Access，单击左下角 Save Changes 按钮，可以看到规则是匹配 Conditions 后执行的 Results，如图 5-13 所示。

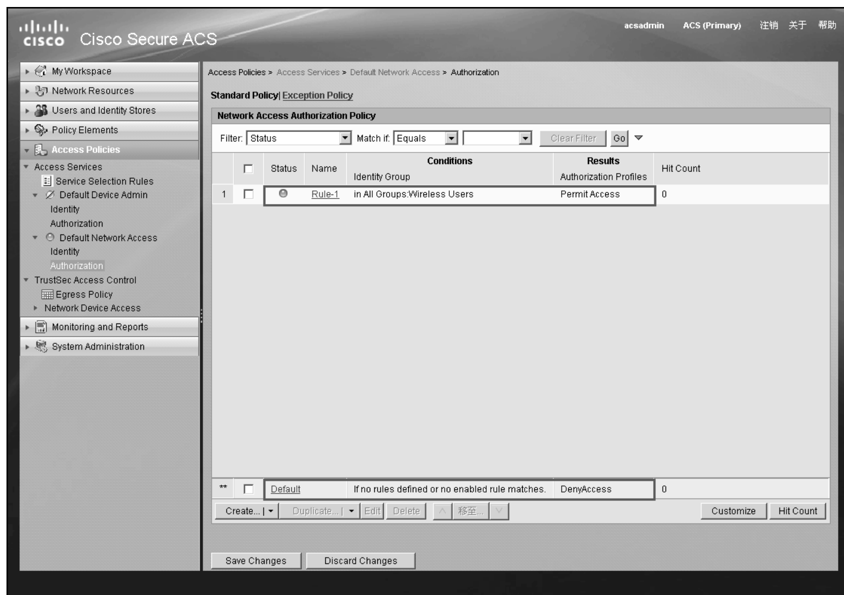


图 5-13　查看授权规则

5.1.2 在 WLC 上配置 RADIUS 服务器相关信息

在 WLC 中选择 Security>AAA>RADIUS>Authentication，单击 New，输入 RADIUS 服务器相关信息，包括服务器地址、共享密钥和认证端口等信息，完毕后单击 Apply 按钮确认，如图 5-14 所示。

图 5-14 在 WLC 上创建 RADIUS 服务器

如果需要对用户的上网信息进行计费，按照上面的做法创建 Accounting Server。

5.2 其他认证方式

RADIUS 是网络设备中最常用的认证方式，除了 RADIUS 认证方式外，本地认证和 LDAP 认证也是目前常见的认证方式。

5.2.1 本地认证服务的创建

本地认证是指用户名与密码都存在本地的用户库中，用户认证是 WLC 通过与本地的用户库比对未完成的，下面讲述如何在 WLC 本地创建用户名与密码。

当进入 WLC 管理界面后，在页面的顶端选择 Security 选项卡，然后在左侧 AAA 菜单中选择“Local Net Users”，如图 5-15 所示。

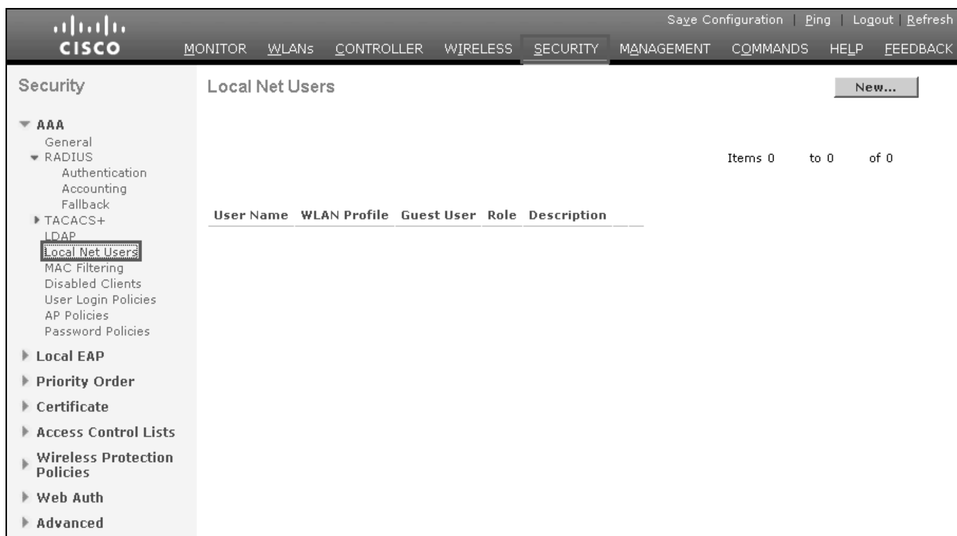


图 5-15　管理本地认证用户

选择 New 创建一个新用户，如 webusers1，密码为 PASSWORD，如果希望此用户只用于特定的 WLAN，可以选择 WLAN 的配置文件，否则先择“Any WLAN”，创建完成后单击 Apply，将用户信息存入库中，如图 5-16 所示。

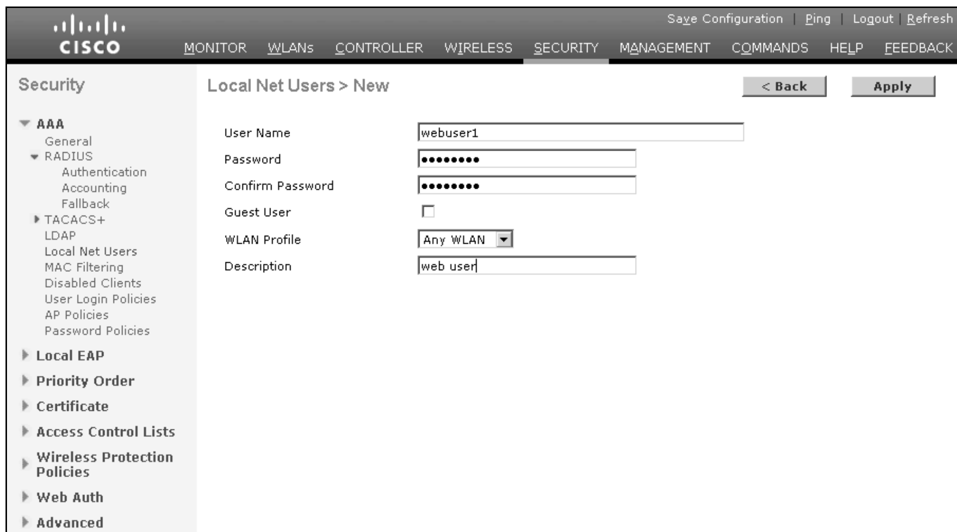


图 5-16　添加本地账户信息

创建完本地账户信息后，还需要创建本地扩展认证协议服务器（Local-EAP Server）。这种服务一般用来在远程办公室中使用，当远程办公室到认证中心的服务器链路中断时，本地控制器可以作为认证服务器来使用。本地 EAP 认证服务包含 LEAP、EAP-FAST 和 EAP-TLS 认证

方式。

当存在全局的外部 RADIUS 服务器时，本地 EAP 认证将不可用；当远程 RADIUS 服务器变得不可用时，本地 EAP 服务将立即生效。

创建 Local-EAP 配置文件，选择 Security > Local EAP Profiles，为该 profile 命名，并在如图 5-17 所示的窗口中选择所有的认证方式。

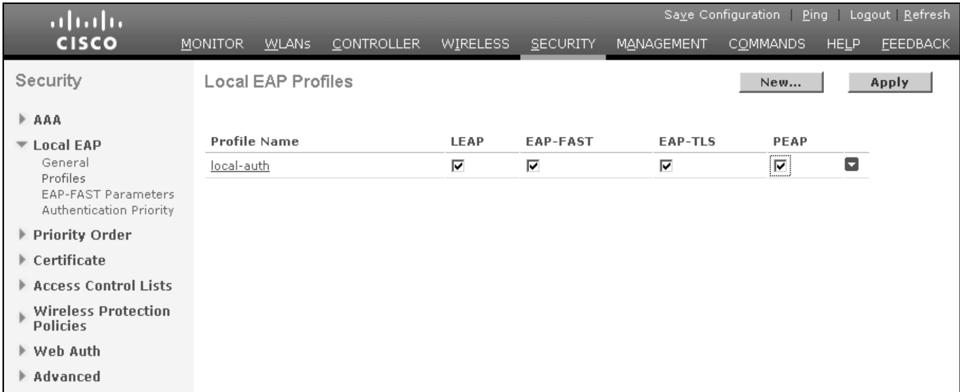


图 5-17　创建本地认证配置文件

如果通过命令行操作，则使用如下的命令：

```
(Cisco Controller) >config local-auth eap-profile method add    leap Local-auth
(Cisco Controller) >config local-auth eap-profile method add    fast Local-auth
(Cisco Controller) >config local-auth eap-profile method add    tls Local-auth
```

可在 Web 管理界面中创建 EAP 的各种参数，这些参数只在 EAP-FAST 中才使用，如图 5-18 所示。

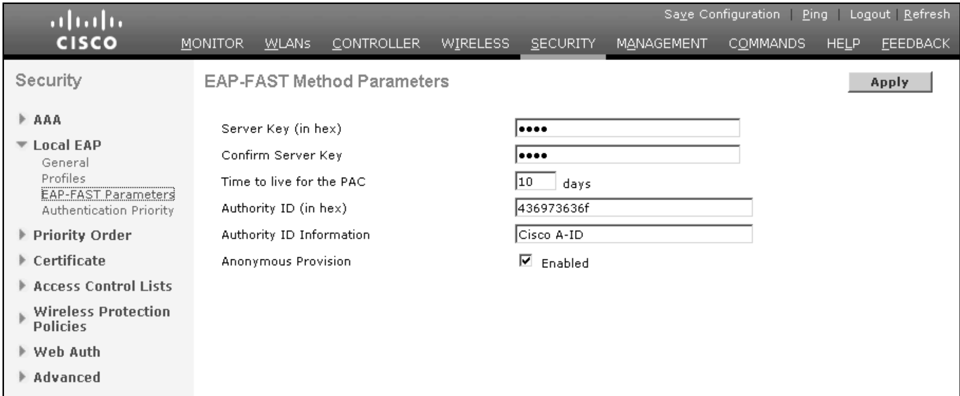


图 5-18　配置 EAP-FAST 认证方式

- Server Key (server-key)：服务器密钥用来加密 / 解密 Protected Access Credentials (PACs)

（用十六进制模式）。

- Time to Live for PAC (pac-ttl)：设置 PAC 的生存期。
- Authority ID (authority-id)：设置授权 ID。
- Annonymous Provision (anon-provn)：配置是否允许匿名授权 AP。

5.2.2　LDAP 认证服务创建

在 WLC 映像软件 5.0 版本以后已经开始支持直接到 LDAP 服务器的认证，而不必经由 ACS 中转，下面详细讲述 LDAP 认证的配置过程。

关于 LDAP 服务器的创建请读者参见相关资料，目前比较流行的 LDAP 服务器为 Windows Acitve Directory Server、Sun Iplanet、Open LDAP 和 Novell EDirectory Server。

下面以 Sun Iplanet 为例，描述 LDAP 服务器配置的过程，如图 5-19 所示。

图 5-19　在 WLC 上创建 LDAP 服务器

如果采用 Windows Acitve Directory Server，用户的属性为 saMAccountName。

5.2.3　MAC 地址过滤

还可以创建基于 MAC 地址过滤的认证方式，用户终端的 MAC 地址只有在认证列表中才能通过系统认证，否则将无法通过认证。MAC 地址认证列表可以在 WLC 内配置，也可以在 RADIUS 服务器配置，后者适合在多控制器环境中部署。当客户端发起连接请求时，WLC 会向 AAA 发送 RADIUS 认证请求，如图 5-20 所示。

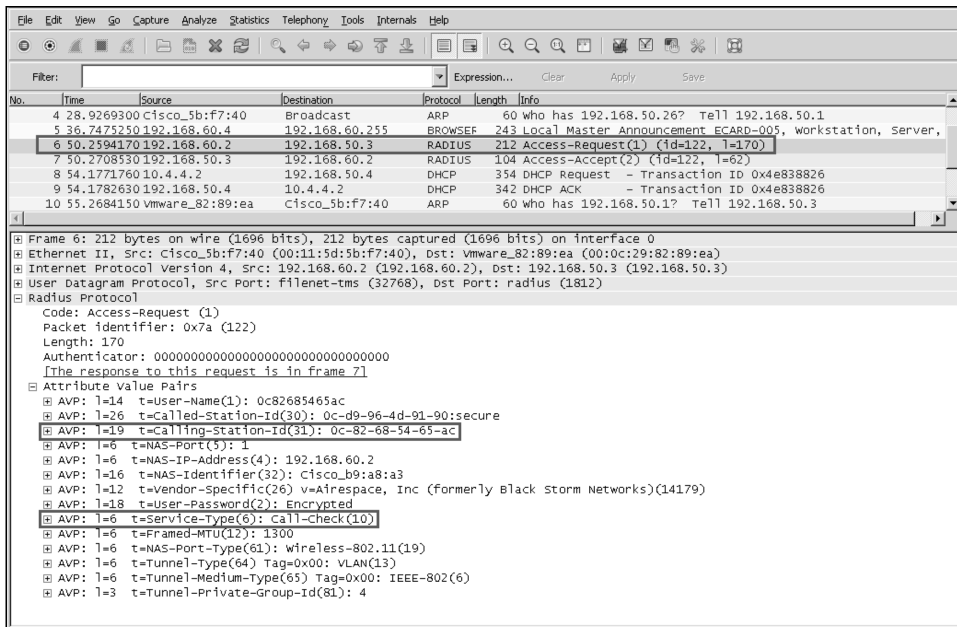


图 5-20 WLC 发送的 RADIUS 认证请求

如果在 WLC 中的 WLAN 勾选了 Layer 2 的 MAC Filtering，那么 ACS 5.x 收到的 RADIUS 请求会包含 Service-Type=10 的属性，ACS 使用请求中的 Calling-Station-Id 属性的值（即 MAC 地址）在身份库（Identity Stores）中进行主机查找（Host Lookup），如果查找到匹配的 MAC 地址，则返回认证通过的 RADIUS 响应。

在 ACS 中配置 MAC 地址过滤服务时需要配置身份库和主机查找策略。身份库可以是 ACS 的本地库，也可以是外部的 LDAP 或者活动目录，此例中配置了 ACS 的本地库。选择 Users and Identity Stores>Internal Identity Stores>Hosts，单击 Create 按钮，创建以 MAC 地址标识的主机，如图 5-21 所示。

主机查找策略的配置可以选择修改默认的 Default Network Access，也可以创建新的访问服务，本例中选择 Access Policies>Access Services，单击 Create 按钮，创建新的访问服务，如图 5-22 所示。

在向导的第一步输入服务名称，选择 Access Service Policy Structure 为 User Selected Service Type，类型为 Network Access，确保勾选 Identity 和 Authorization 前面的复选框，单击下一步按钮。

在向导的第二步默认已经勾选了 Process Host Lookup，然后单击 Finish 按钮，如图 5-23 所示。

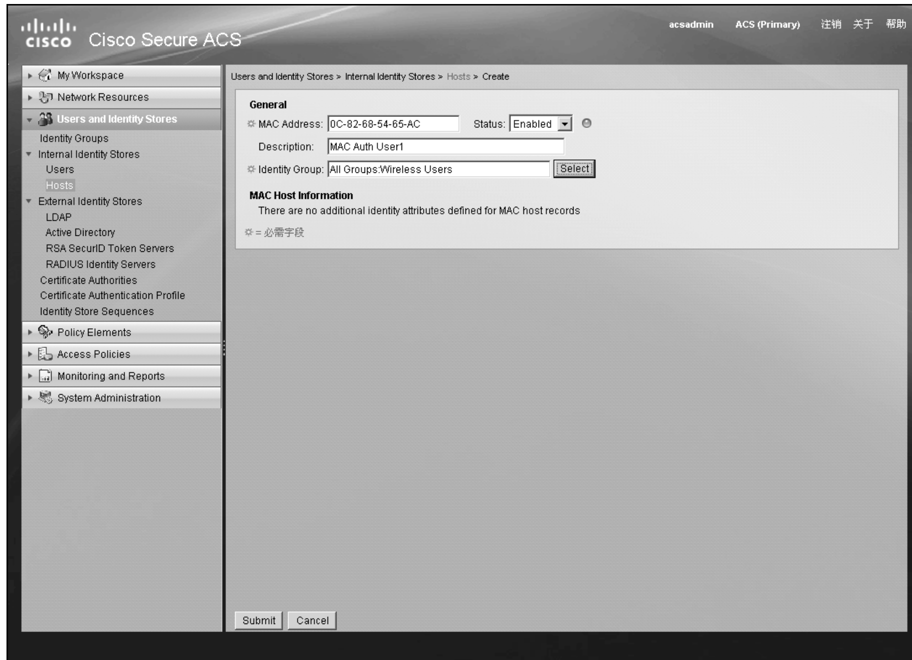


图 5-21　配置主机身份库

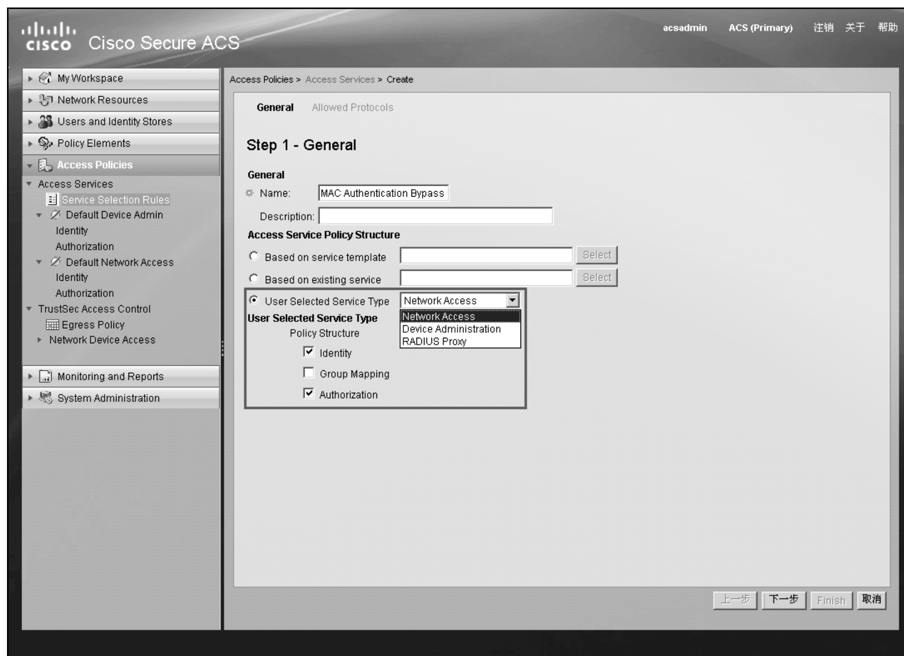


图 5-22　创建访问服务向导

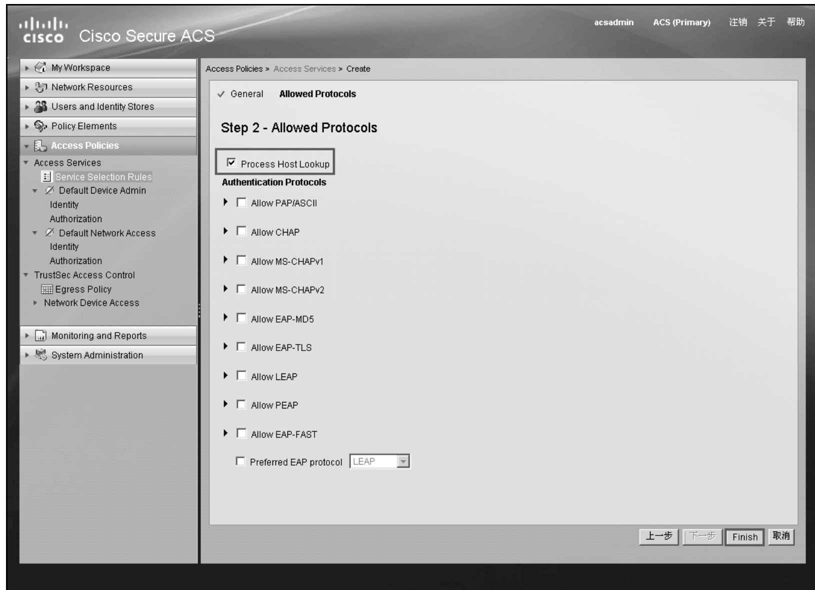


图 5-23　访问服务中的主机查找

创建好访问服务后，选择 Access Policies>Access Services>Service Selection Rules，勾选 Single result selection 并在 Service 下拉框中选择之前创建的访问服务来处理 RADIUS 请求，然后单击 Save Changes 按钮，如图 5-24 所示。

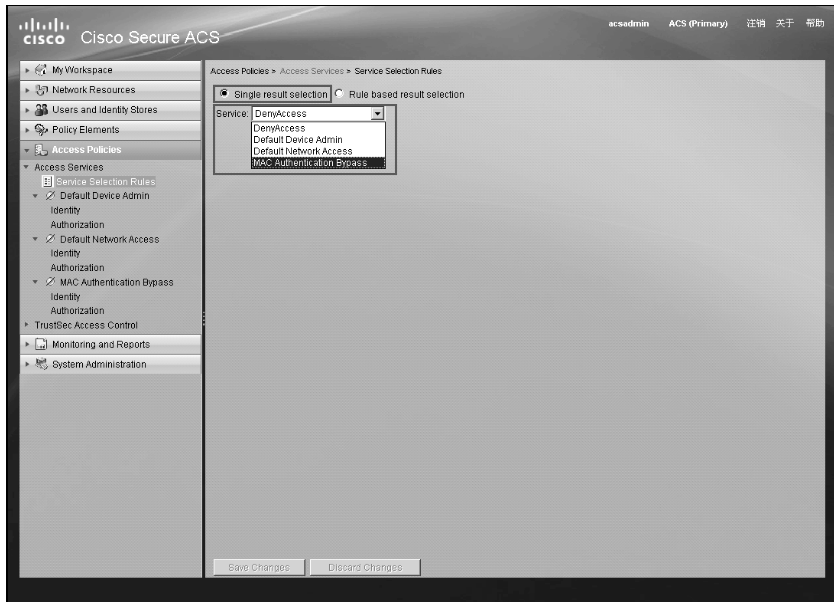


图 5-24　定义 RADIUS 请求的处理方式和服务

选择 Access Policies>Access Services>创建的访问服务>Identity，选择 Identity Source 的默认值 DenyAccess 为 Internal Hosts，如图 5-25 所示。

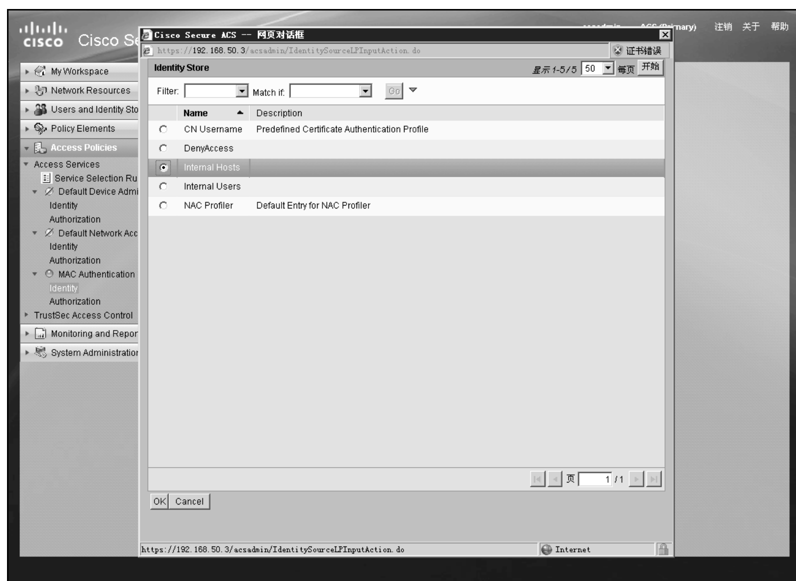


图 5-25　定义认证服务的认证源

选择 Access Policies>Access Services>创建的访问服务>Authorization，单击 Customize 按钮，选择 UseCase 作为规则条件，选择 Authorization Profiles 作为规则结果，然后单击 OK 按钮，如图 5-26 所示。

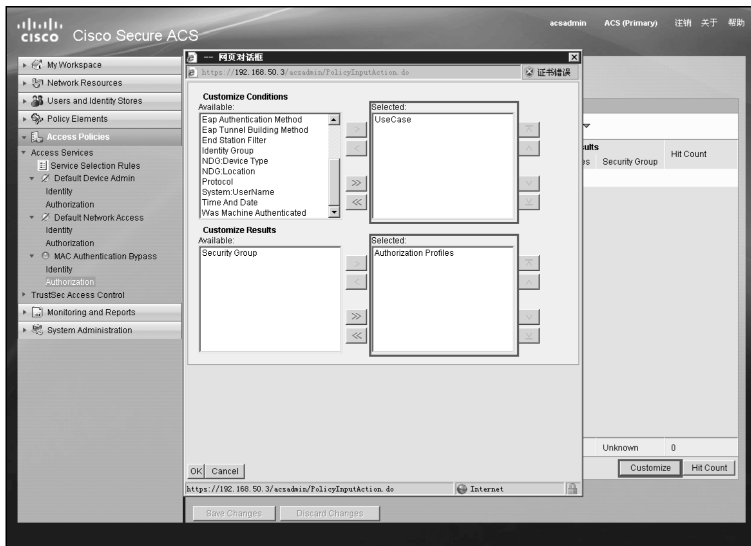


图 5-26　定义规则的条件与结果

回到 Access Policies>Access Services>创建的访问服务>Authorization 界面，单击 Create 按钮，选择规则条件 UseCase 匹配 Host Lookup，规则结果为 Permit Access，如图 5-27 所示。

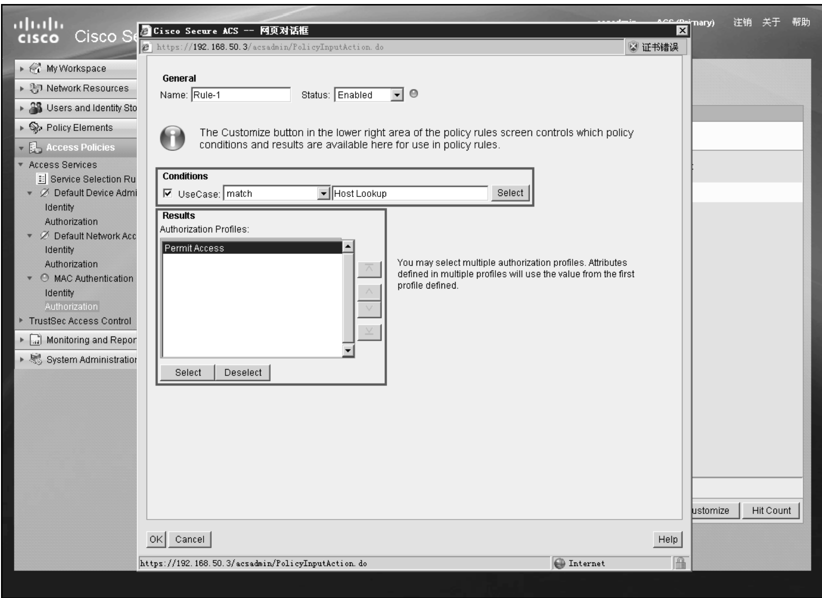


图 5-27　创建 Host Lookup 规则

最后单击 Default 规则，修改认证失败的结果为 DenyAccess，如图 5-28 所示。



图 5-28　修改默认规则

MAC 地址过滤可以同其他认证方式同时使用，以增强安全性。在 WLC 中的 WLAN 可以不勾选 Layer 2 的 MAC Filtering，虽然发送的 RADIUS 请求中 Service-Type=2，但也带了 Calling-Station-Id 的属性，所以可以在 ACS 5.x 中配置 End Station Filters 作为一个规则条件来基于 MAC 地址过滤认证请求。

选择 Policy Elements>Session Conditions>Network Conditions>End Station Filters，单击 Create 按钮，输入 MAC 地址过滤列表的名字并选择 MAC Address 标签页，如图 5-29 所示。

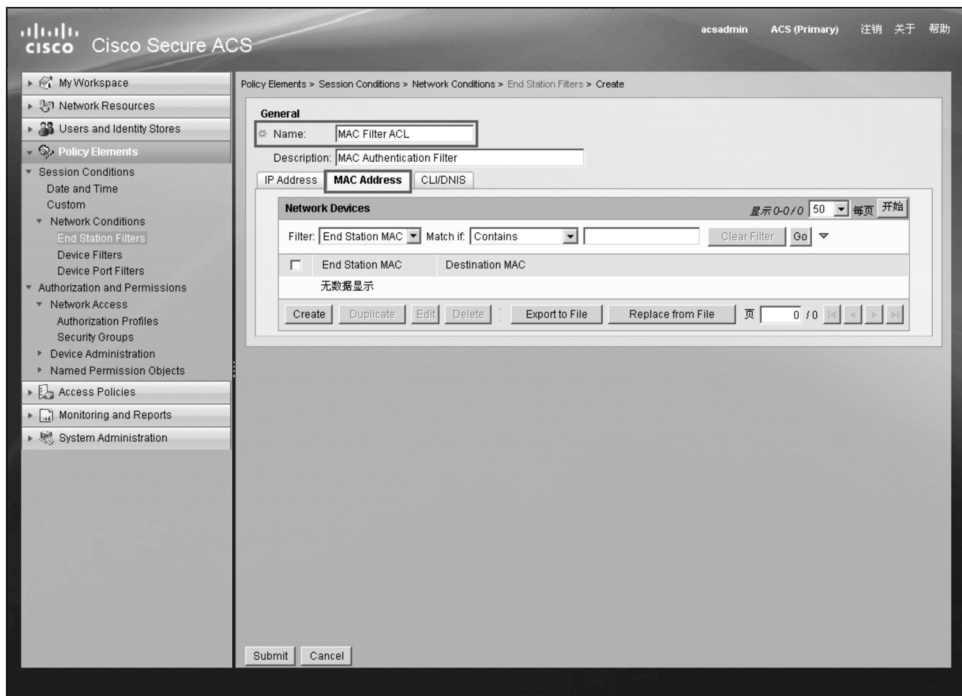


图 5-29　添加 MAC 地址认证列表

单击 Create 按钮，在弹出的添加 MAC 地址对话框中，勾选 End Station MAC 并输入用户终端的 MAC 地址，然后单击 OK 按钮，如图 5-30 所示。

添加完 MAC 地址后，单击 Submit 按钮提交。创建的 MAC 地址过滤列表可以作为身份库选择规则条件，也可以作为授权规则条件。

5.2.4　配置 WLAN 使用各种认证服务

选择 WLANs>Edit ’secure’>Security>AAA Servers，选择各种认证方式，并从最下方选择各种认证方式的次序，如图 5-31 所示。

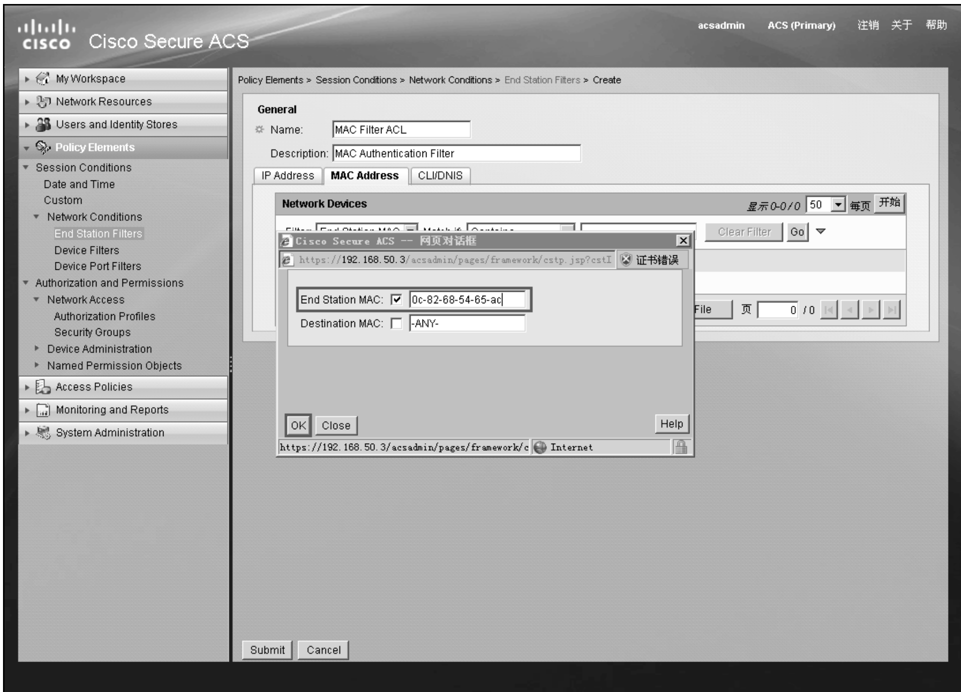


图 5-30 添加用户终端的 MAC 地址



图 5-31 配置 WLAN 的认证服务器

5.3 创建 Guest 账户

控制器可以在 WLAN 上提供 Guest 的访问权限，为了创建 Guest 账户，必须首先创建大堂经理账户，Cisco 内部叫大堂大使账户（Lobby Ambassador），一旦创建了此账户，大堂大使就可以在控制器上创建和维护 Guest 用户账户信息。大堂大使只能使用 Web 页面管理用户账户，

且只有有限的配置权限。

大堂大使可以指定账户的生存周期，一旦指定的时间过去，相应的 Guest 账户将会自动被销户。本地用户账户的条目最多只有 2 048 条，一般被设置为 512 条默认值（在 Security > General Page 中），本地库包含的账户有：本地管理账户（包含大堂大使账户）、本地网络用户（包含 Guest 账户）、MAC 地址过滤条目和被禁止的用户，这些用户的总和不能突破 2 048 条数据库的大小。

5.3.1　创建大堂大使账户

导航到 Management > Local Management Users 增加本地管理账户，单击 New 创建大堂大使账户，选择 User Access Mode 为 LobbyAdmin，输入用户名与密码，单击 Apply 按钮，就可以创建大堂大使账户，如图 5-32 所示。

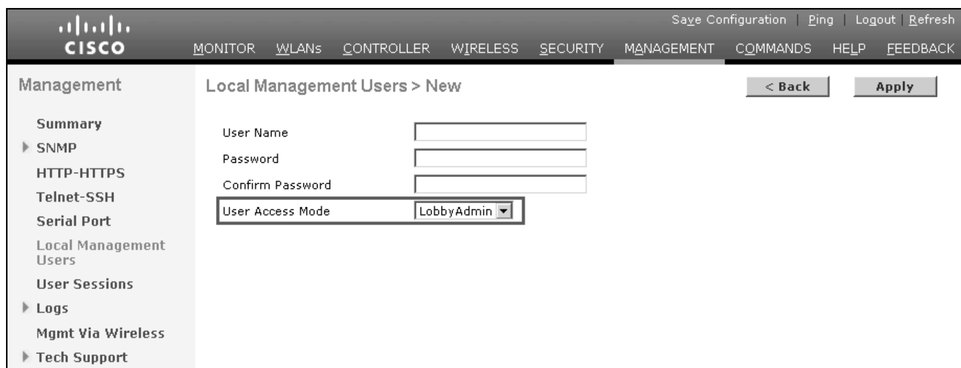


图 5-32　添加大堂大使账户

5.3.2　使用大堂大使账户创建 Guest 账户

使用创建的大堂大使账户登录 Web 管理界面，单击 New，创建新的 Guest 账户，输入用户名、密码（可以让系统产生随机的密码）以及生存期，选择合适的 WLAN SSID（可供选择的 WLAN 只能是采用第三层认证方式），最后单击 Apply 按钮即可创建相关用户。用户的生存时间为 5 分钟到 1 个月，如图 5-33 所示。

5.3.3　配置有线来宾访问

有线来宾访问允许来宾用户通过有线网络访问相应的资源，有线来宾访问端口可能会在一些来宾办公室或会议室，同无线来宾账户一样，有线来宾账户也可以通过大堂大使创建。有线

来宾账户通过有线网络端口连接到网络，有线网络端口再通过无线控制器进行终结，从而对用户的访问进行认证及授权，有线来宾的网络访问如图 5-34 所示。

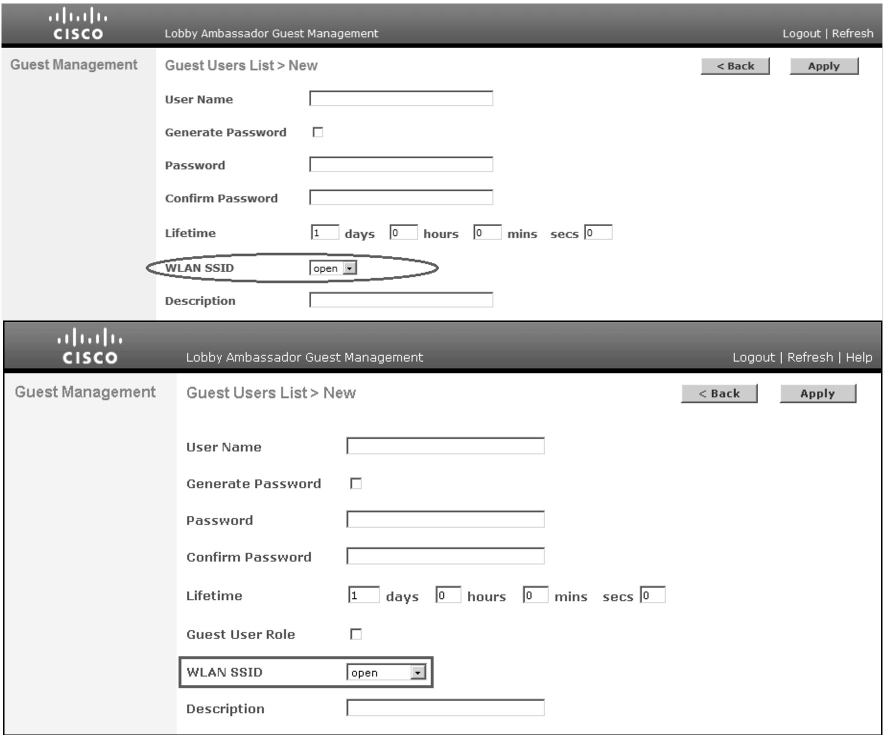


图 5-33　使用大堂大使账户创建 Guest 账户

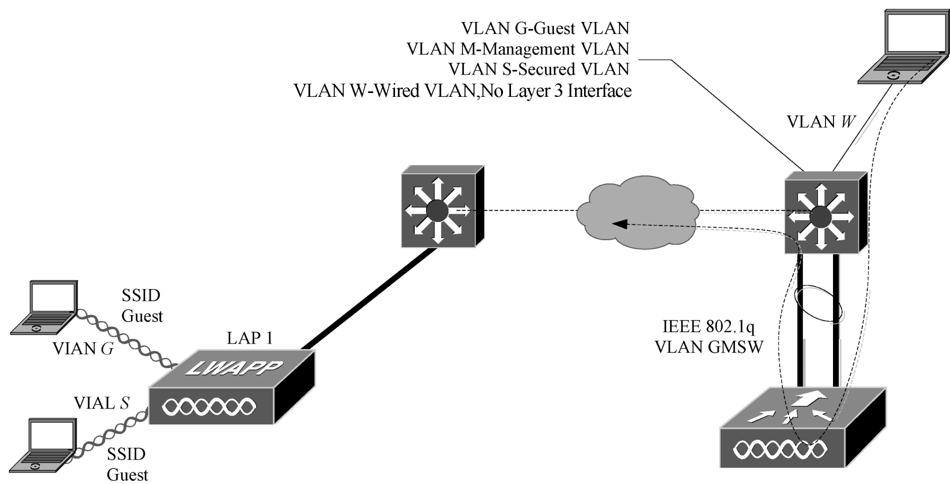


图 5-34　配置有线来宾账户拓扑图

设置的步骤如下：

① 在多层交换机上创建有线 VLAN *W* 供有线访客使用，此 VLAN 不能创建对应的第三层接口。

② 在控制器上创建一个动态 Guest VLAN 接口供有线访客使用，其 VLAN ID 同上一步中的 ID 必须相同。

③ 在多层交换机上创建另一个 VLAN *G*，并为之设置第三层接口，配置 DHCP 地址池，以便此接口通过 WLC 分配 IP 地址给 VLAN *W* 中的用户。

④ 在控制器上创建另外一个动态接口，此 VLAN ID 为 *G*，指定接口地址、掩码、网关及 DHCP 服务器等信息。

⑤ 在控制器上创建一个 Wired WLAN 同动态接口相关联，进口指定为②中配置的端口，出口配置为④中配置的端口。

⑥ 配置 Wired-WLAN 所用的认证方式。

下面讲述使用 Web 管理界面配置 WLC。

① 导航到 Controller > Interfaces，单击 New，创建一个新接口，给接口命名，并指定 VLAN ID，将 Guest LAN 的复选框选中，指定合适的端口号码，单击 Apply 按钮，如图 5-35 所示。

图 5-35　配置 Guest LAN 接口

② 创建另外一个动态接口 Guest LAN，输入相应的 IP 地址、掩码、网关以及 DHCP 服务器地址，详细的配置方法此处不再赘述。

③ 创建 WLAN，导航到 WLAN，在下拉框选中 Create New，单击 Go，开始新建 WLAN；

在 Type 的下拉列表选择 Guest LAN，输入配置文件名称，如图 5-36 所示。



图 5-36　配置 Guest WLAN

④ 单击 Apply，在接下来的界面中指定虚拟输入输出端口，输入端口指定为 Wired-Guest，输出端口指定为 Guest LAN，选中 Status 边上 Enabled 的复选框，单击 Apply 按钮，如图 5-37 所示。



图 5-37　配置 Guest WLAN 的状态及进出端口

Guest LAN 不再支持第二层的认证，第三层认证采用 Web Authentication 或 Web Passthrough，并可以指定 AAA 认证方式或在本地认证。当配置完毕后，将计算机插入交换机 VLAN *W*（就是 Wired-Guest 接口中创建的 VLAN）接口，计算机将会自动获得 VLAN *G*（Guest LAN 所在的 VLAN）的 IP 地址；当访问未授权的 URL 时，系统将会自动弹出 Portal 页面让用户认证。

第6章 

管理无线网络控制器

本章要点

- WCS及其配置
- 升级控制器软件
- 管理控制器配置文件
- 清除控制器配置文件
- 重新启动控制器

6.1 WCS 及其配置

Cisco 无线控制系统 （Wireless Control System，WCS）是业内最全面的管理平台，用于对 IEEE 802.11n 和 IEEE 802.11a/b/g 企业级无线网络的生命周期进行管理。这一强大的管理平台可提供经济高效的管理解决方案，使 IT 管理员可以成功地规划、部署和监控室内和室外无线网络的情况，并排除故障和定制报告。

6.1.1 WCS 简介

作为思科统一无线网络的管理平台，Cisco WCS 是支持高性能的应用程序和关键任务的解决方案，可简化业务运营程序并提高生产效率。该系统还支持 Cisco CleanAir 技术，这项技术是思科统一无线网络的系统级功能，它使用硅片级智能创建自行恢复和自行优化的无线网络。Cisco CleanAir 技术在为 IEEE 802.11n 网络提供性能保护的同时，通过自动减缓射频（RF）干扰的影响，提高无线网络的可靠性，支持关键任务应用程序的运行。

Cisco WCS 是一个全面的平台，伸缩自如，可满足跨本地、远程、国内和国际位置的大中小型无线局域网的各种需求。此项获奖的解决方案可使 IT 经理在需要时立即使用所需的工具，只要从一个集中位置便可实施和维护安全的无线局域网，不仅效率更高，而且最大限度地减少了 IT 人员配备。

Cisco WCS 直观的用户界面和使用简易的内置工具，可提高 IT 人员的效率，降低 IT 人员的培训成本，最大限度地降低对 IT 人员配备需求，从而显著降低运营成本，即使网络不断扩展也是如此，如图 6-1 所示。与重叠管理工具不同的是，Cisco WCS 通过将全方位管理需求（包括射频、控制器和服务）结合到单个统一平台来降低运营成本。

Cisco WCS 是新老 IT 管理员理想的管理平台。对需要自动化管理体验的用户来说，Cisco WCS 简单直观的用户界面可降低复杂性，而全面的生命周期管理功能可满足最高级 IT 管理员的需求。Cisco WCS 内在的灵活性使每位用户都能够定制管理界面，仅显示达成运营目标和业务目标所需的最相关信息。

Cisco WCS 以经济高效的方式支持无线局域网生命周期的各个阶段，从规划和部署到监控，乃至故障排除和定制报告。Cisco WCS 使无线局域网的运行在生命周期的各个阶段都更加有效和高效，如图 6-2 所示。

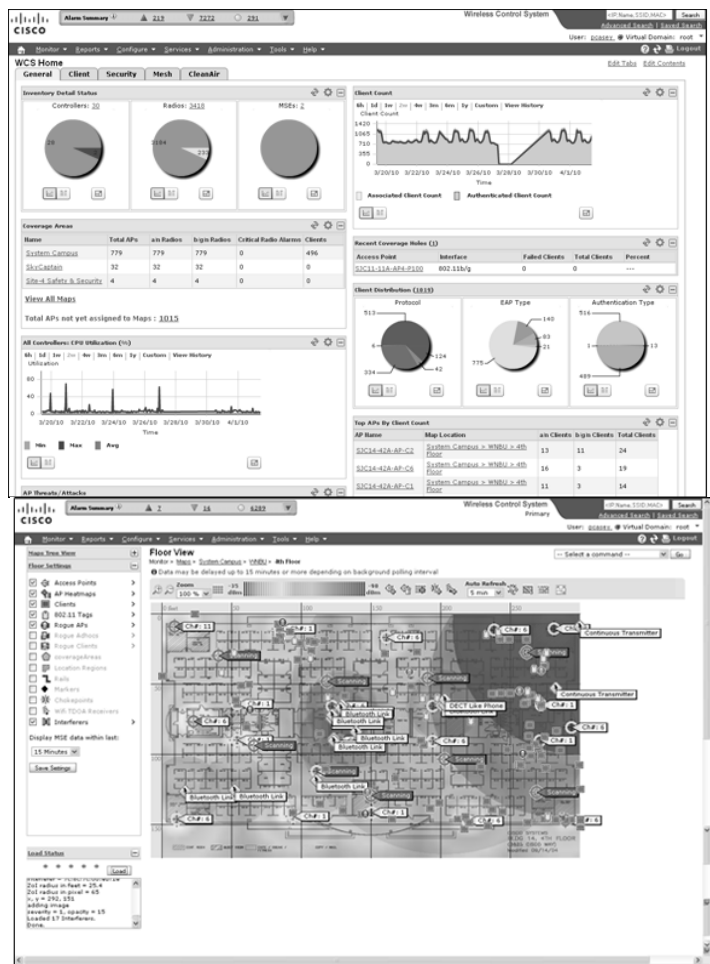


图 6-1　WCS 监控界面

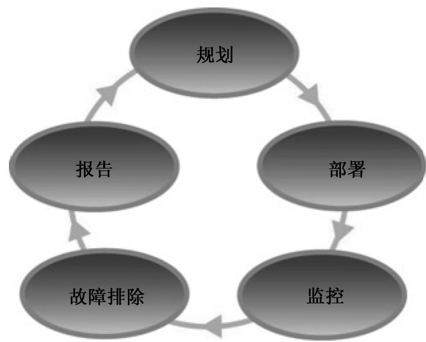


图 6-2　WCS 的对无线局域网各方面的管理

通过 Cisco WCS 的内置规划和设计工具套件，可以使有效支持关键业务数据、语音和视频服务的无线局域网设计得以简化，如图 6-3 所示。

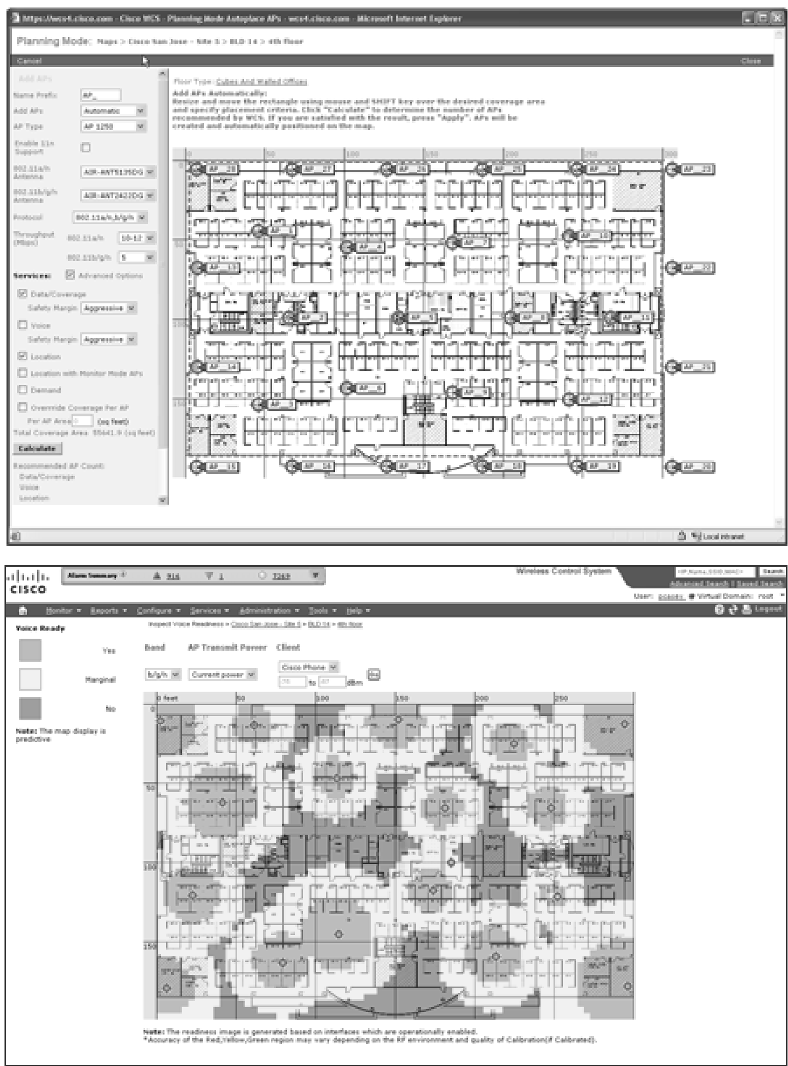


图 6-3 简化的无线局域网规划和设计

Cisco WCS 规划和设计工具可简化以下流程：针对标准建筑和形状不规则的建筑，定义无线接入点的布局并确定无线接入点的覆盖区域。这些工具可以使 IT 管理员清楚地了解射频环境，从而更容易显现理想的射频环境、预期未来的覆盖需求和评估无线局域网活动。这些工具可帮助 IT 管理员减少（在许多情况下甚至是消除）不适当的射频设计和覆盖问题，避免产生最终用户故障通知单。

专业化的 Cisco WCS 规划工具支持对无线局域网就绪性进行直接评估，以支持无线局域网上的语音服务和环境感知（位置）服务。无线局域网上的语音服务支持具备 WiFi 功能的单模和双模电话。环境感知服务与思科移动服务引擎相结合，可使用户能够使用思科正在申请专利的“射频指纹”技术查找、跟踪和管理具备 WiFi 功能的设备及其环境信息。

通过众多的 Cisco WCS 集成配置模板简化流程，无线局域网可以快速投入使用，经济高效地满足最终用户的需求。这些易于使用的模板和部署工具可帮助 IT 经理调配和配置无线局域网，明确提供其业务所需的服务。

通过易于使用的界面，可以获得 Cisco WCS 灵活的模板，这使得跨一个或多个无线局域网控制器使用常用配置变得非常简单。无须考虑这些控制器在网络中的位置，无论它们是与 Cisco WCS 位于同一局域网、位于单独的路由子网还是跨广域网连接都一样。只需单击一个按钮，IT 管理员便可简化整个无线网络最为复杂的控制器配置、更新和调度。通过可支持单个或多个无线接入点定制配置的易用模板，自动设置无线接入点也同样简单。灵活的部署工具和配置模板如图 6-4 所示。

Cisco WCS 是一个理想的管理平台，可用于监控整个无线局域网，以维持卓越性能并向移动最终用户提供最佳无线体验。Cisco WCS 的集中化界面使得根据需要或预定随时随地访问信息变得非常简单，如图 6-1 所示。

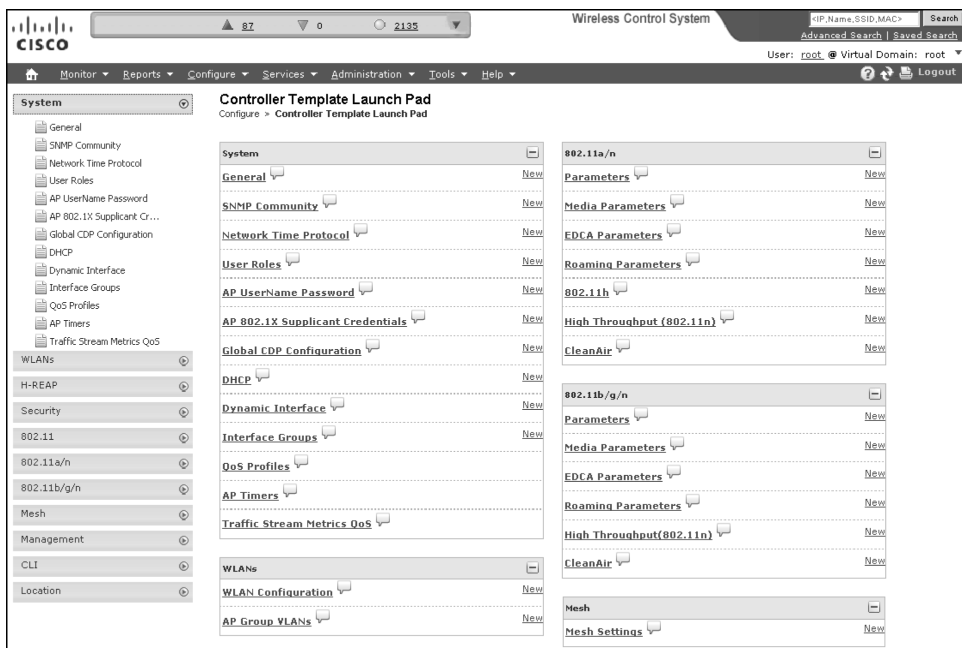


图 6-4　灵活的部署工具和配置模板



图 6-4　灵活的部署工具和配置模板（续）

Cisco WCS 易于使用的图形显示可作为维护、安全、故障排除和未来能力规划活动的起点。通过各种入口点，可以快速访问有关网络中出现的正常和不正常事件的可操作数据，这使得 Cisco WCS 对于持续的网络运行至关重要。

Cisco WCS 中持久可用的警报摘要简化了基于严重性对关键信息、故障和警报的访问，便于更快地评估重要通知并快速解决问题通知单。当启用了位置服务时，完全支持检测、定位和控制未经授权（欺诈）设备的功能。持久可用的警报摘要和简化的欺诈设备检测与定位如图 6-5 所示。

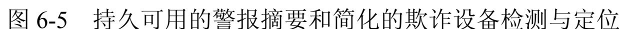


图 6-5　持久可用的警报摘要和简化的欺诈设备检测与定位

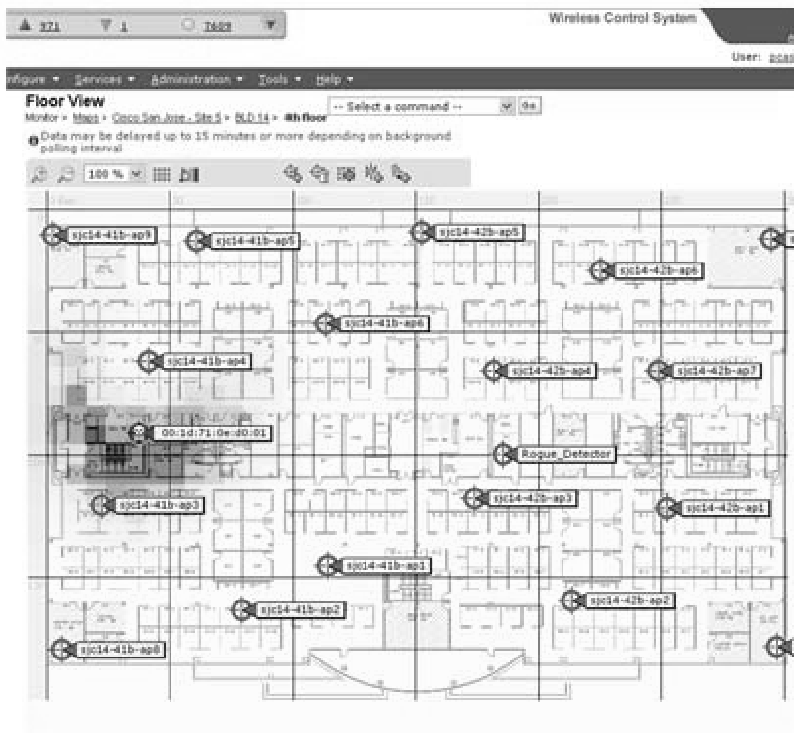


图 6-5　持久可用的警报摘要和简化的欺诈设备检测与定位（续）

Cisco WCS 的集成工作流和大量故障排除工具可帮助 IT 管理员快速确定、隔离和解决思科统一无线网络所有组件中出现的问题。Cisco WCS 支持在 IT 人员配备最少的情况下，对任何规模的无线局域网进行快速故障排除。

Cisco WCS 便于快速评估服务中断，接收有关性能降低的通知，研究解决办法，采取行动来补救非最佳状况。集成的工作流支持在所有基础设施组件和客户端设备的所有工具、警报、警告、搜索和报告之间进行无缝连接。

各种工具配合使用，可帮助 IT 管理员了解无线局域网上出现的细微运行差别，发现基准参数之外的非最佳活动。例如，客户端连接或漫游问题。Cisco WCS 中持久可用的搜索工具便于跨网络访问无线网络中任意位置的设备和资产的相关即时信息和历史信息。如需清楚地了解射频性能、状态统计和空气介质质量，可以使用射频资源管理（RRM） 和空气介质质量信息，如图 6-6 所示。

Cisco CleanAir 技术支持查找、分类、关联，减少来自 WiFi 和非 WiFi 的干扰源，如欺诈无线接入点、微波炉、蓝牙设备和无绳电话等。Cisco CleanAir 可提高空气介质质量，创建自行恢复和自行优化无线网络，从而减缓无线干扰源的影响，如图 6-7 所示。

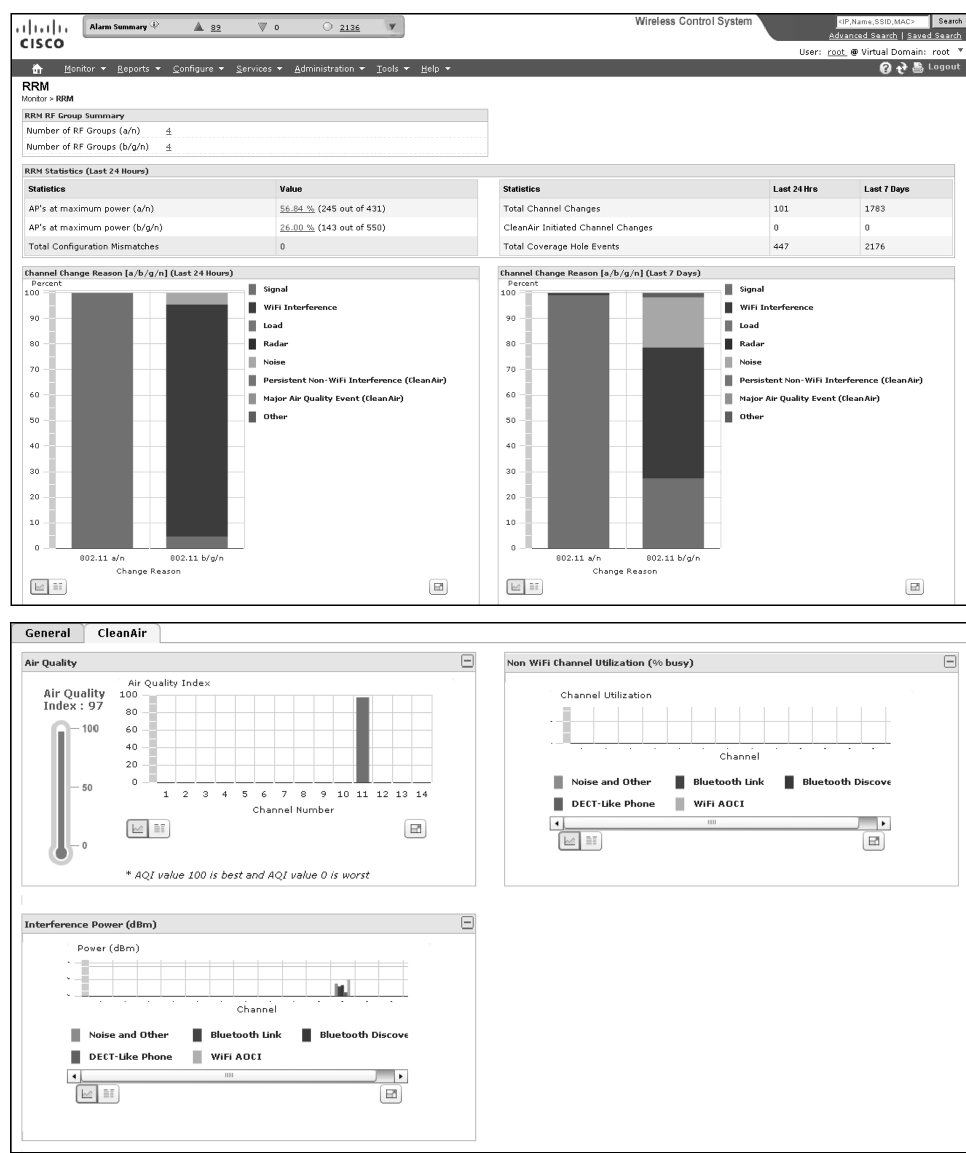


图 6-6　内置射频资源管理和空气介质质量评估

内置客户端故障排除工具提供分步方法，能为所有客户端设备分析故障。此工具通过加快解决各种 WiFi 客户端设备类型的问题通知单来降低运行成本。这一强大的客户端故障排除工具还可以协助进行客户端趋势分析。当使用思科兼容扩展（Cisco Compatible Extensions）客户端和 Cisco CleanAir 技术时，专业化诊断工具可用于支持连接问题的深入分析，如图 6-8 所示。

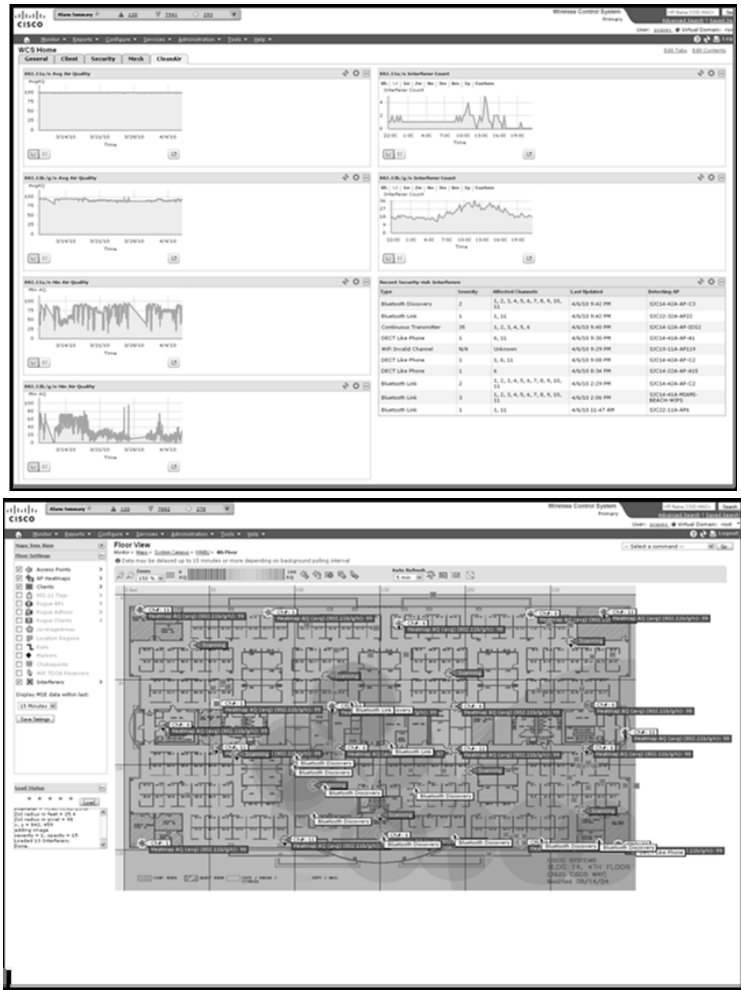


图 6-7　Cisco CleanAir 技术

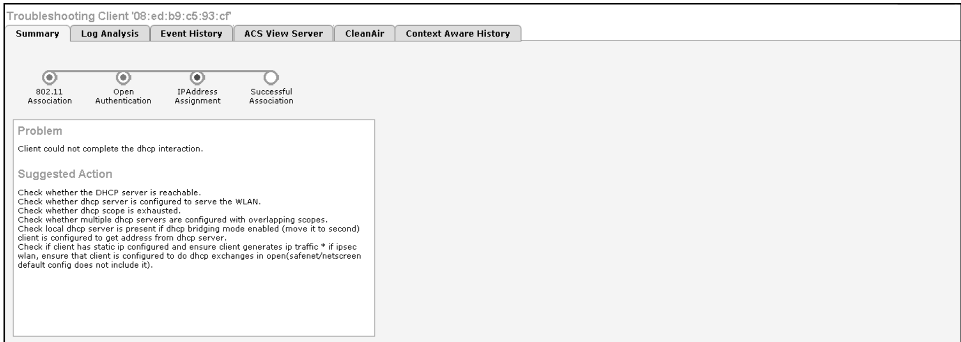


图 6-8　内置客户端故障排除工具支持分步问题分析

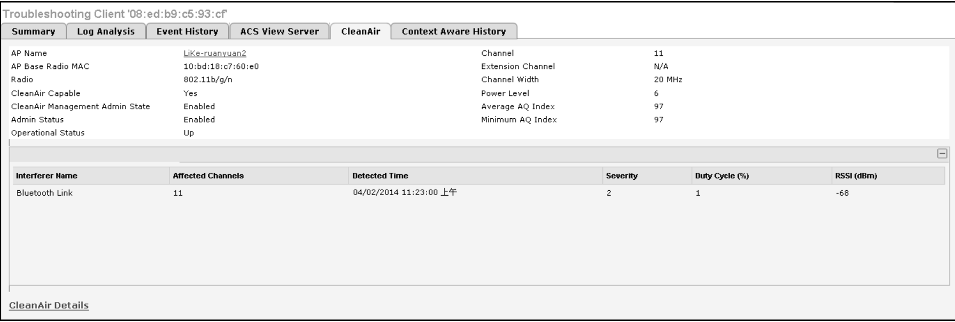


图 6-8　内置客户端故障排除工具支持分步问题分析（续）

Cisco WCS 包括可定制的报告，用于协助 IT 团队更有效地管理、维护和不断发展无线局域网，以满足持续的业务需求和运营需求。灵活的报告可用于在适当的时间，以满足任何需求的方式，访问适当的数据，如图 6-9 所示。

各种各样的报告可用来帮助 IT 经理立足前沿，随时掌握网络发展趋势，保持对网络的控制，审核运营状况并快速应对不断变化的业务需求和最终用户需求；可根据用户定义的参数来定制报告，通过从数个报告收集数据并分析趋势以了解无线局域网随时间发生的变化，可简化对任意位置和时间的网络运行状况的详细分析以及能力规划，了解无线局域网趋势，使得对未来增强与发展的规划变得更加轻松。

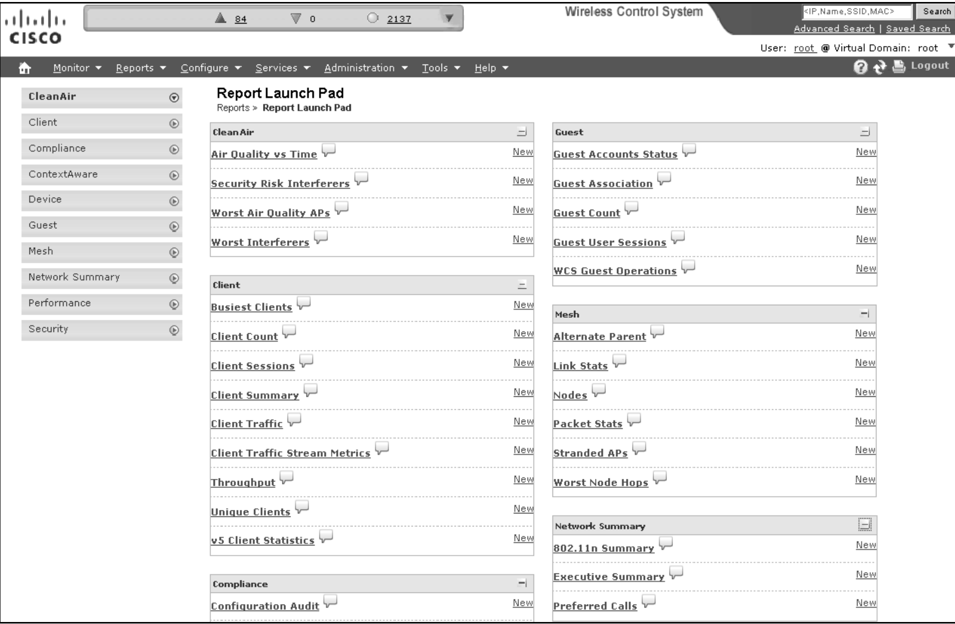


图 6-9　可定制的报告满足任何需求

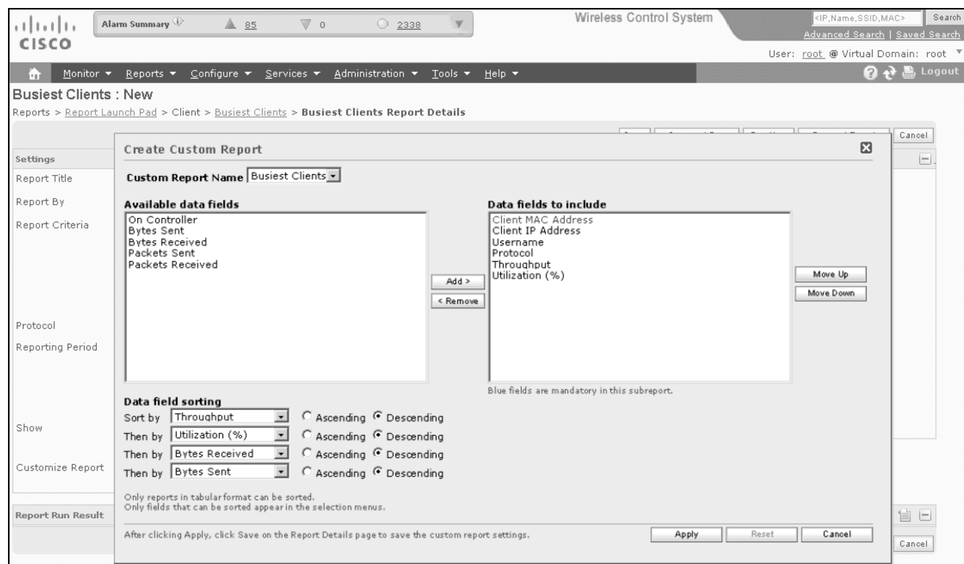


图 6-9　可定制的报告满足任何需求（续）

6.1.2　使用 WCS 规划热图

在 WCS 中可以采用地图对 AP 进行定位，同时对 AP 进行规划。导航到 Monitor>Maps，即可查看所有的 Map 信息，其中包括了园区、大楼及楼层等信息。每张图中包含 AP 总数、IEEE 802.11a 和 IEEE 802.11b/g 的数量，以及告警信息、用户数量和状态信息等，如果需要对显示的信息进行修改，可以单击 Edit View，修改需要显示的栏目信息。

如果需要增加一张地图，可以从右上角的 Command 菜单中选择新建园区地图或大楼地图，也可以通过命令菜单添加、修改和删除地图信息。

如果有精确的地图数据，如 CAD 图纸，我们可以先创建园区图，园区图仅支持图片格式，我们需要将相应的模式转化成.bmp、.jpg 和.png 等图片格式，并确定图纸以英尺为单位的真实大小（1 米长度约为 3.28 英尺），WCS 还支持以 GPS 坐标标注图纸，这样可以标注 AP 及用户的准确位置，WCS 还支持从 Google Earth 实时导入地图数据。当园区图创建完成后，可以创建下一层图纸，包括大楼及室外空间，在创建大楼图纸时，需要指定大楼的层数和地下层数，拖动选择框可以确定大楼在园区图中的位置。室外空间需要上传图片格式的图纸，同时指定 AP 的高度，确定后即可以在园区图纸中选择相应的区域。

如果没有园区图而直接增加大楼图纸，可以直接指向左侧 Maps Tree View>Maps>Root Area 增加大楼信息。

在大楼信息完成后，需要按照每层楼添加相应的楼层图纸，楼层图纸支持从 CAD 到 PNG 等图片格式的转换，如图 6-10 所示，在增加楼层图纸时，需要提供楼层名称和联系人，选择

层数、墙体的类型和楼层高度，最后是楼层的 CAD 图。

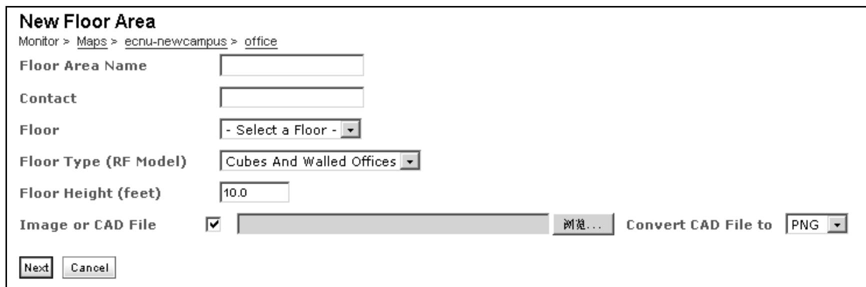


图 6-10　在 WCS 中增加楼层图纸

在楼层图导入完成后，可以通过 Map Editor 修改图纸信息，包括增加墙体及门的信息，因为这些障碍物会对无线信号产生一定的衰减；在墙体和门增加完毕后，需要向楼层图纸中增加合适的 AP，如图 6-11 所示。

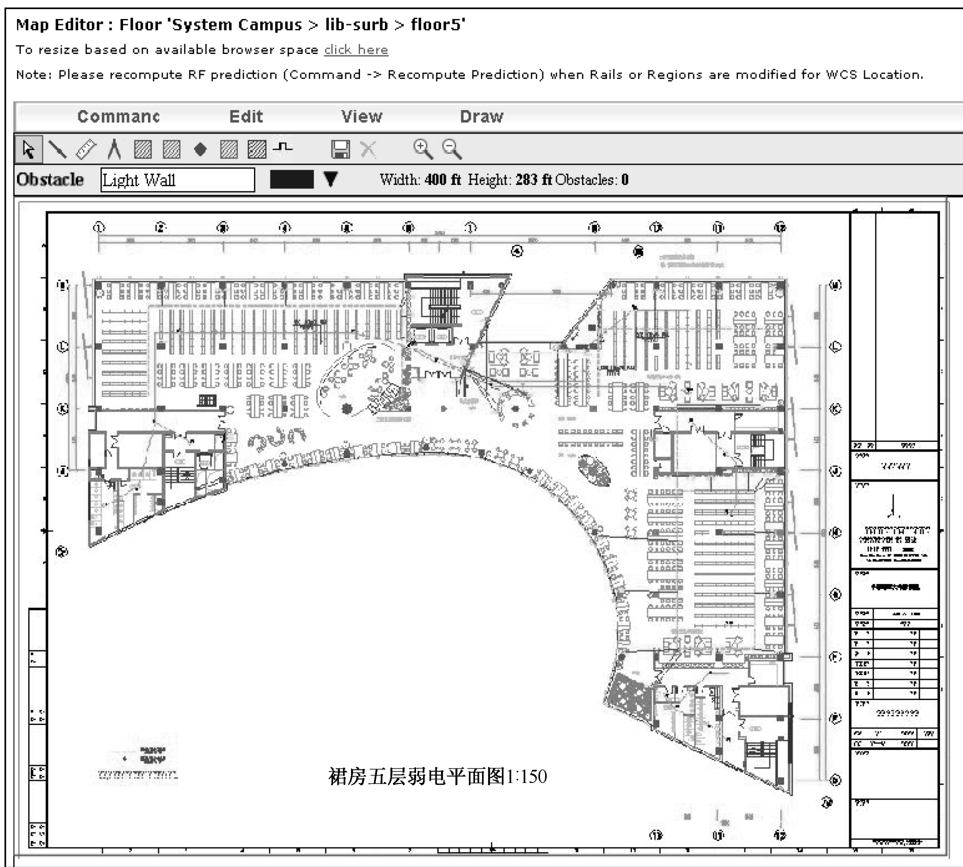


图 6-11　向楼层图纸中增加 AP

从命令列表中选择 Add Access Points，从 AP 列表中选择相应的 AP，选择完成后，单击 OK 确认。接下来再从命令列表中选择 Position AP，对每个 AP 进行定位，包括 AP 的水平、垂直位置、高度和天线的仰角等信息。

当定位完成后，可以看到图 6-12 所示的 AP 热图，在热图中可以选择显示 AP 的名称、MAC 或用户数等信息，如果购买了 Cisco 的定位系统，还可以对每个用户进行准确的定位。

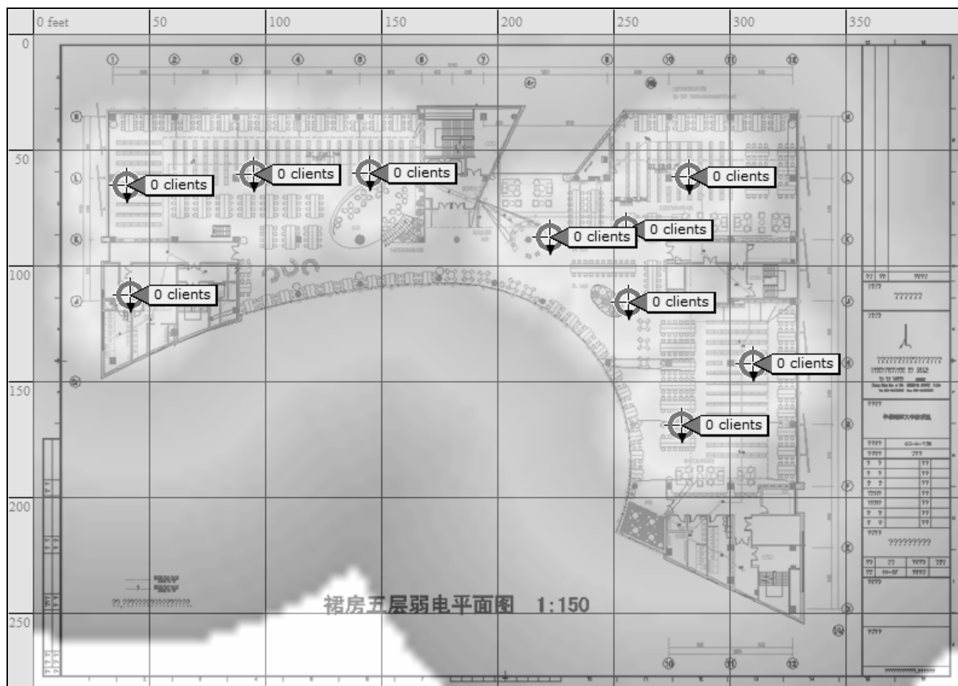


图 6-12　楼层 AP 热图显示

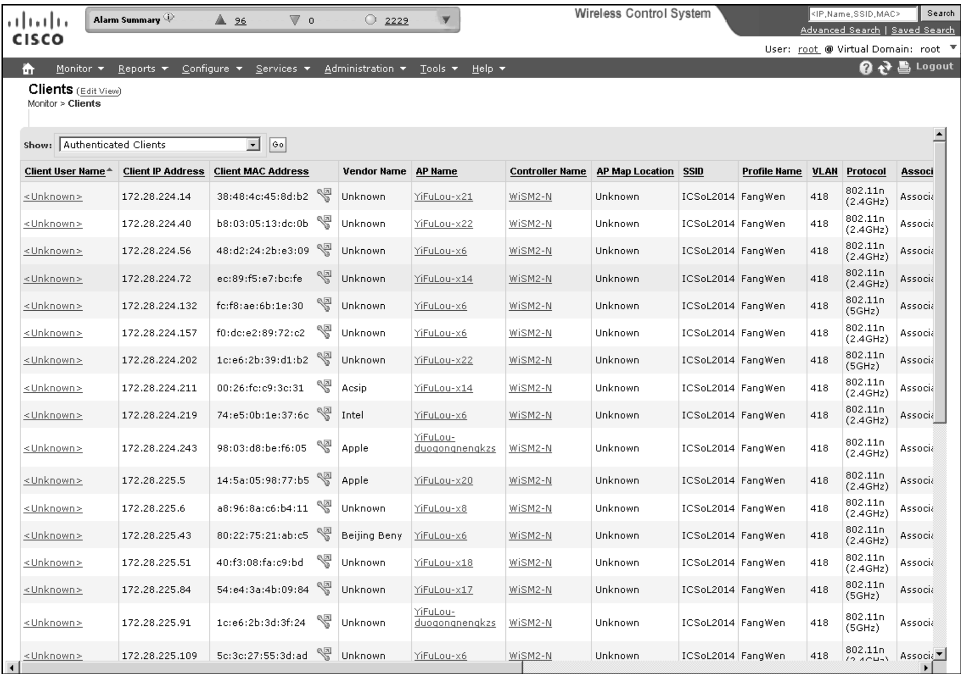
6.1.3　使用 WCS 查看接入用户的信息

从 WCS 中可以查看关联的用户信息，包括用户的数量、使用的认证方式及用户的流量等，图 6-13 是关于用户的信息，左侧的饼图显示了用户使用的认证方式及各种认证方式所占的百分比，右上部分显示按时间分布的用户数量，右下部分显示用户的流量信息。

单击相应认证方式的饼图，即可查看采用此种方式的所有用户列表，列表中包含了用户名、IP 地址、MAC 地址、连接的 AP 名称和控制器信息等详细的信息，如图 6-14 所示。



图 6-13　WCS 中用户信息查看



Client User Name	Client IP Address	Client MAC Address	Vendor Name	AP Name	Controller Name	AP Map Location	SSID	Profile Name	VLAN	Protocol	Associ
<Unknown>	172.28.224.14	38:48:4c:45:8d:b2	Unknown	YiFuLou-x21	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.40	b8:03:05:13:dc:0b	Unknown	YiFuLou-x22	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.56	48:d2:24:2b:e3:09	Unknown	YiFuLou-x6	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.72	ec:89:f5:e7:bc:fe	Unknown	YiFuLou-x14	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.132	fc:f8:ae:6b:1e:30	Unknown	YiFuLou-x6	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (5GHz)	Associ
<Unknown>	172.28.224.157	f0:dc:e2:89:72:c2	Unknown	YiFuLou-x6	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.202	1c:e6:2b:39:d1:b2	Unknown	YiFuLou-x22	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (5GHz)	Associ
<Unknown>	172.28.224.211	00:26:fc:c9:3c:31	Acsip	YiFuLou-x14	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.219	74:e5:0b:1e:37:6c	Intel	YiFuLou-x6	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.224.243	98:03:d8:be:f6:05	Apple	YiFuLou-duogongnengkzs	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.225.5	14:5a:05:98:77:b5	Apple	YiFuLou-x20	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.225.6	a8:96:8a:c6:b4:11	Unknown	YiFuLou-x8	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.225.43	80:22:75:21:ab:c5	Beijing Beny	YiFuLou-x6	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.225.51	40:f3:08:fa:c9:bd	Unknown	YiFuLou-x18	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (2.4GHz)	Associ
<Unknown>	172.28.225.84	54:e4:3a:4b:09:84	Unknown	YiFuLou-x17	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (5GHz)	Associ
<Unknown>	172.28.225.91	1c:e6:2b:3d:3f:24	Unknown	YiFuLou-duogongnengkzs	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n (5GHz)	Associ
<Unknown>	172.28.225.109	5c:3c:27:55:3d:ad	Unknown	YiFuLou-x6	WiSM2-N	Unknown	ICSoL2014	FangWen	418	802.11n	Associ

图 6-14　采用 WCS 查看用户详细信息

单击 Link Test 可以测试客户端与 AP 之间的链路状况，如图 6-15 所示。

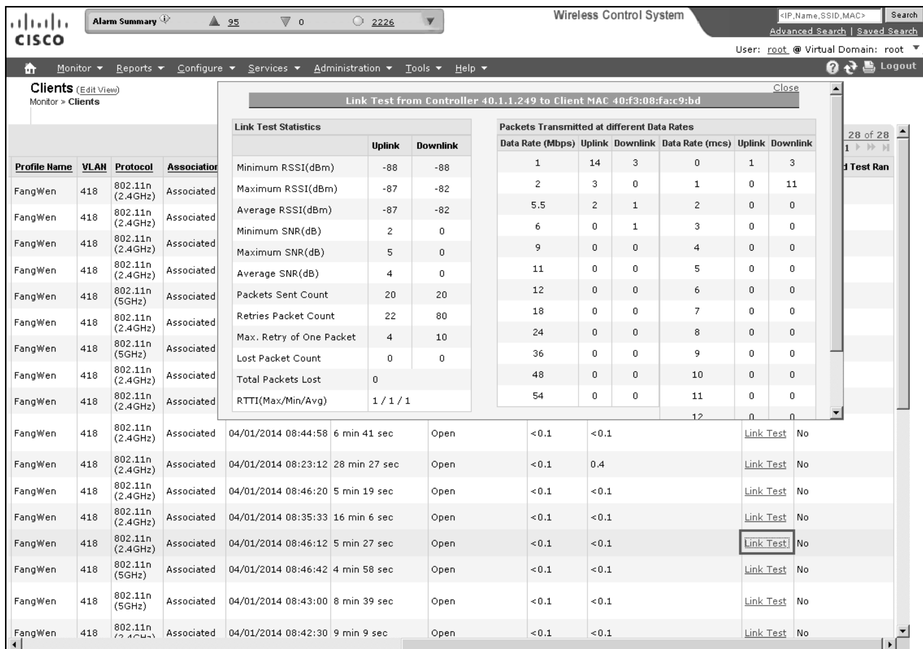


图 6-15　采用 WCS 测试用户的无线链路

回到主页面，单击右上角 Edit Contents，可以向主页面中增加监控的信息，如图 6-16 所示。



图 6-16　更改 WCS 的显示栏目

可增加的内容包括用户分布、用户流量和用户的事件警告等，如图 6-17 所示。

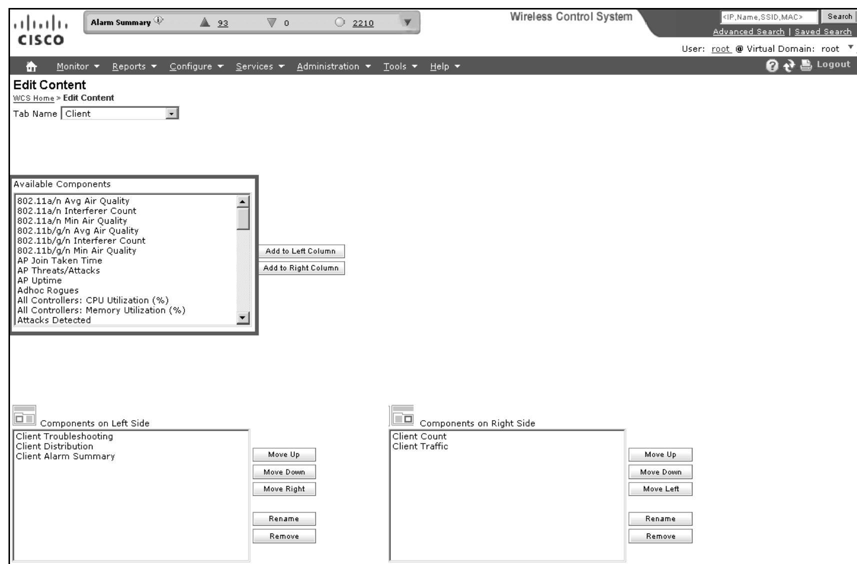


图 6-17　可选择的显示类别

导航到 Monitor>Clients，可以看到所有的用户信息，包括同 AP 关联的和没有关联的用户，选择 Show 的下拉列表即可以根据特定的条件对用户进行筛选，例如，使用 2.4 GHz 频率的用户、所有认证通过的用户、所有列入黑名单的用户等，如图 6-18 所示。

Alarm Summary 91 0 2194　Wireless Control System

Clients (Edit View)
Monitor > Clients

Show: Associated Clients　Go

---Select client filter---
2.4GHz Clients
5GHz Clients
All Clients
Associated Clients
Authenticated Clients
Clients detected by MSE
Clients detected in last 24 hours
Excluded Clients
H-REAP Locally Authenticated
New Clients detected in last 24 hours
Probing Clients
Unauthenticated Clients
WGB Clients

Client User	IP Address	MAC Address	Vendor Name	AP Name	Controller Name	AP Map Location	SSID	Profile Name	VLAN	Protocol	Association
<Unknown>		:2d:e6:08	Unknown	HouQin-7	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>		d0:88:f6	Unknown	Lib-main-floor3.1	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>		b0:27:bb	Unknown	math2	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>		:b2:1c:47	Asotel	HouQin-5	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>		44:05:d2	Unknown	AP0011.bb5a.49ba	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.24.139	04:fe:31:d8:b7:d5	Unknown	math-V	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.30.53	b8:5e:7b:8b:48:79	Unknown	AP0011.bbba.8e5e	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.66.234	ec:89:f5:d8:ef:bc	Unknown	Teacher-Center-I	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.71.139	70:11:24:97:08:09	Unknown	HouQin-7	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.128.17	1c:af:05:5f:20:9a	Unknown	AP0011.bb47.3694	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.129.187	64:b3:10:fc:99:58	Unknown	HouQin-7	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.130.48	48:d2:24:1c:93:b5	Unknown	math2	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.144.165	b0:9f:ba:df:10:08	Unknown	HouQin-7	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.145.157	88:32:9b:c5:31:18	Unknown	HouQin-7	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.145.165	ec:89:f5:42:32:7c	Unknown	HouQin-2	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.146.65	9c:20:7b:27:de:91	Unknown	Lib-main-floor3.1	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.146.215	f4:6d:e2:cb:71:72	Unknown	math2	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated
<Unknown>	172.29.146.237	04:db:56:4f:ef:dd	Unknown	Lib-main-floor1.2	Wism-I	Unknown	ECNU	ECNU	416	802.11g	Associated

图 6-18　用户详细信息显示

单击 MAC 地址右边的工具按钮，可以诊断用户的各种状态，包括对用户的认证过程进行记录以取得相关的日志信息，供排错使用，如图 6-19 所示。

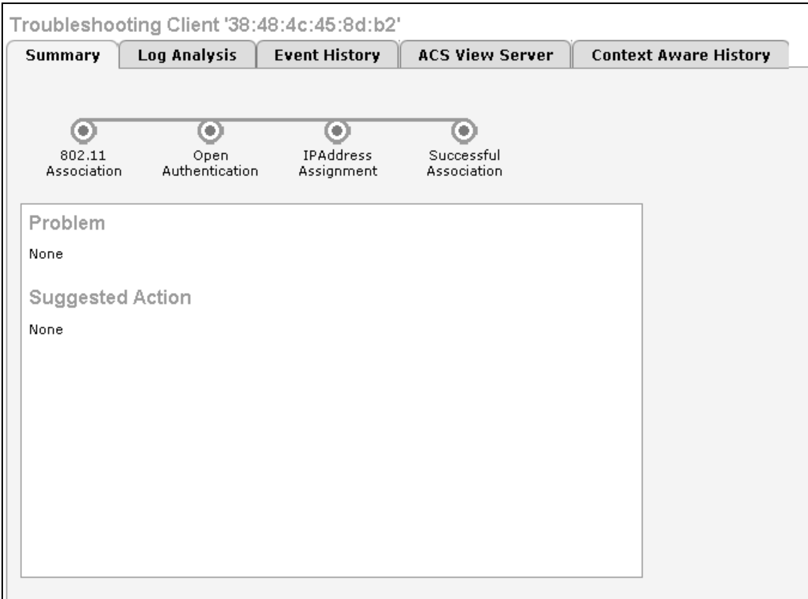


图 6-19　用户的故障排除

单击用户名，即可以查看此用户的详细信息，包括用户的关联历史记录、历史收发报文数量和历史信号质量信息等，如图 6-20 所示。

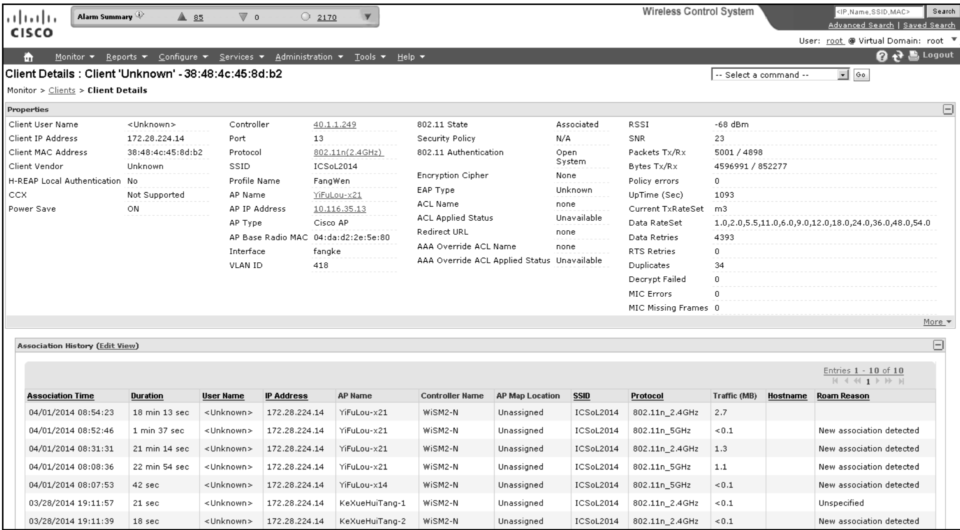


图 6-20　用户的实时及历史信息查看

还有一种根据 AP 查询用户的方法，导航到 Monitor>Access Points，单击任意一个 AP，在 AP 的详细信息中，选择 Current Associated Clients，即可查看同此 AP 关联的所有用户信息，如图 6-21 所示。

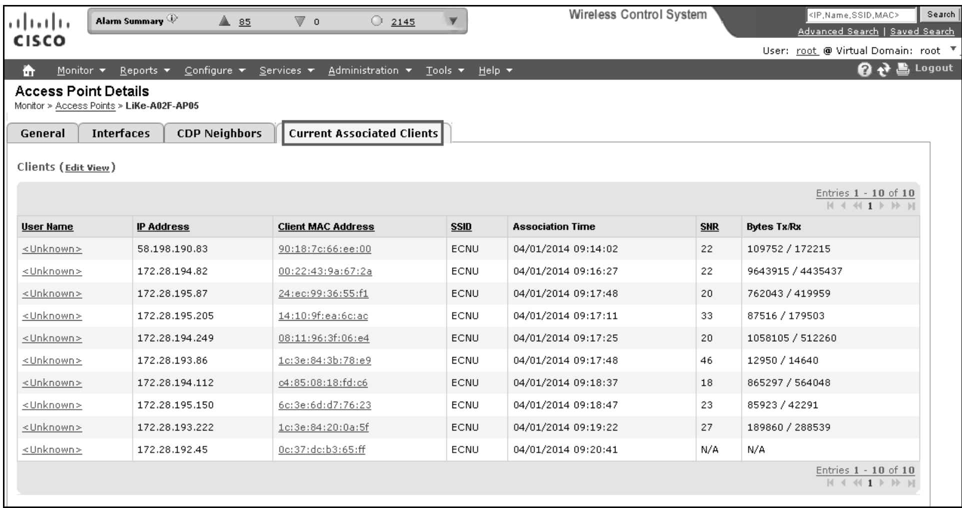


图 6-21 查看 AP 关联的用户信息

如果希望查找特定用户的信息，可以直接在顶端查找框中输入用户名、IP 地址、MAC 地址或 SSID，都可以查找用户信息。在返回的结果列表中，单击 Client 行所在的 View List，即可以查看这些用户的信息，如图 6-22 所示。

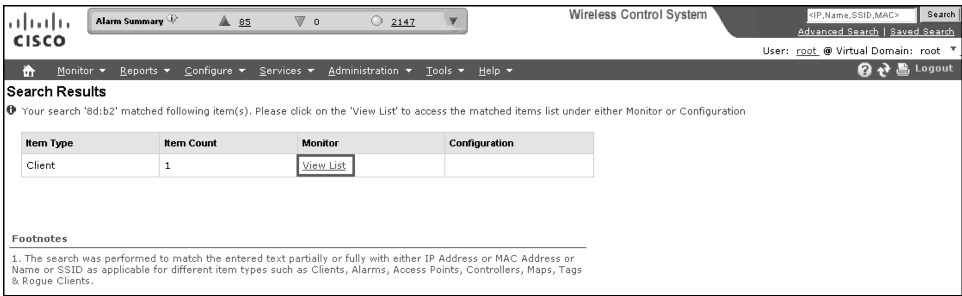


图 6-22 在搜索框中查找用户的信息

6.1.4 使用 WCS 自定义报表

Cisco WCS 提供了多种报表功能，共分为 Clean Air、Client、Compliance、Device、Guest、Mesh、Network Summary、Performance 和 Security 九种功能（最新软件版本 7.0 下）。每一大类功能中包含了很多子功能的报表，例如，Device 功能下包含了 Busiest APs 和 Utilization 等子

报表功能。下面我们以 Busiest APs 为例，介绍报表功能的使用。

导航到 Reports>Report Launch Pad，选择 Devices>Busiest APs，选择 New，新建一个报表，如图 6-23 所示，填写报表的名称以及按照何种类型分类（按照控制器还是按照地图）、对何种协议进行统计及统计周期等，完毕后选择 Save and Run。

图 6-23 自定义报表

将会出现如图 6-24 所示的列表，按照使用率从高到低进行排列。

Report Run Result

Busiest-AP-Test

Wireless Control System

Generated: Tue Apr 01 09:43:00 CST 2014

Report By: AP By Controller
Protocol: 802.11b/g/n
Reporting Period: Last 366 days
Show: Up to 50 records

Busiest APs

AP Name	Radio Type	Rx Utilization (%)	Tx Utilization (%)	Channel Utilization (%)	Controller Name
HeKouSuo-East-4F-42	802.11b/g/n	0.00	1.67	73.92	WiSM2-N
Like-B218-III	802.11b/g/n	0.00	1.00	73.00	WiSM2-N
HeKouSuo-West-6F-78	802.11b/g/n	0.00	1.42	70.58	WiSM2-N
HeKouSuo-East-3F-33	802.11b/g/n	0.00	1.50	69.75	WiSM2-N
HeKouSuo-West-6F-80	802.11b/g/n	0.00	1.42	69.33	WiSM2-N
HeKouSuo-East-5F-43	802.11b/g/n	0.00	1.67	68.83	WiSM2-N
HeKouSuo-East-5F-46	802.11b/g/n	0.00	2.33	68.67	WiSM2-N
Like-B218-I	802.11b/g/n	0.00	2.00	68.00	WiSM2-N
HeKouSuo-East-6F-51	802.11b/g/n	0.00	1.75	67.58	WiSM2-N
LiKe-ruanyuan1	802.11b/g/n	0.00	1.09	66.94	WiSM2-N
HeKouSuo-West-4F-68	802.11b/g/n	0.00	1.50	65.83	WiSM2-N

Page 1 of 4

图 6-24 使用报表显示最忙的 AP 信息

还可以针对此报表安排一个计划任务，让报表周期性运行。对那些使用率很高的 AP，可以在其周边增加 AP 的部署；对那些常年使用率很低甚至基本没人使用的 AP，可以拆除或减少周边 AP 的部署，以达到资源的优化使用。

6.2 升级控制器软件

当升级控制器映像软件时，与之对应的 LAP 的映像软件也将同时被升级。当 LAP 正在升级软件时，LED 的灯将交替闪烁，一个控制器可同时升级 10 个与之关联的 LAP。

升级软件之前，必须准备好升级使用的 TFTP 或 FTP，升级一般使用 Management 端口，如果使用 Service Port，则 TFTP 或 FTP 服务器所在的网段必须同服务端口在同一个网段，因为服务端口不能进行路由操作。由于最新的映像软件都已经超过 32 MB，当使用 TFTP 软件时，必须保证 TFTP 服务器支持 32 MB 以上的软件映像文件，否则将会出现“TFTP failure while storing in flash”的错误信息。

6.2.1 使用 Web 管理页面升级 WLC 映像软件

在 Web 管理界面中可以通过如下的步骤升级映像软件。

① 将 WLC 的配置文件上传到 TFTP 或 FTP 服务器中。

② 将控制器映像软件置于 TFTP 或 FTP 合适的目录之下。

② 在控制器上禁用所有 IEEE 802.11a/b/g 无线信号。

③ 如果是对 WiSM 升级，先在交换机上禁用 port channel，以防止在重新启动前 LAP 下载相关软件。

⑤ 在控制器上禁用所有的 WLANs。

⑥ 单击 Commands > Download File 命令，打开“Download file to Controller”页面，如图 6-25 所示。

图 6-25 Download file to Controller 页面

⑦ 在 File Type 下拉列表中选择 Code，在 Transfer Mode 中选择 TFTP，完成相应的路径名和映像文件名称，如果选择 FTP 方式，还必须输入 FTP 服务器的用户名与密码。

⑧ 单击 Download 按钮开始向控制器下载映像软件。

⑨ 下载完成后，单击 Reboot。

⑩ 如果系统要求用户保存配置，选择 save and reboot。

⑪ 单击 OK 确定，并重新启动控制器。

⑫ 控制器重启完成后，重新使能所有的 WLANs。

⑬ 如果是 WiSM，重新开启 port channel 功能。

⑭ 重新使能所有 IEEE 802.11a/b/g 信号。

⑮ 如果不确定，可以重新下载控制器的配置文件。

⑯ 在 Monitor>summary 页面确认系统的软件版本是否正确。

6.2.2　使用 CLI 命令端口升级控制器软件

使用命令行端口升级 WLC 的映像软件可以使用如下的步骤。

① 将 WLC 的配置文件上传到 TFTP 或 FTP 服务器中。

② 将控制器映像软件放置于 TFTP 或 FTP 合适的目录之下。

③ 在控制器上禁用所有 IEEE 802.11a/b/g 无线信号。

④ 如果是对 WiSM 升级，在交换机上禁用 port channel，以防止在重新启动前 LAP 下载相关软件。

⑤ 登录到控制台接口，在控制器上禁用所有的 WLANs，采用 config wlan disable *wlan_id* 命令。

⑥ 确认是否可以顺利连通（通过 Ping 命令）TFTP 或 FTP 服务器软件。

⑦ 输入 transfer download start 并采用 n 回答，查看当前的下载参数配置。

```
Mode.......................................... TFTP
Data Type..................................... Code
TFTP Server IP................................ xxx.xxx.xxx.xxx
TFTP Packet Timeout.............................. 6
TFTP Max Retries................................. 10
TFTP Path..................................... <directory path>
TFTP Filename................................. xxx.aes
This may take some time.
Are you sure you want to start? (y/N) n
Transfer Canceled
```

⑧ 如有必要，输入如下命令更改下载配置。

```
transfer download mode {tftp | ftp}
transfer download datatype code
transfer download serverip server-ip-address
transfer download filename filename
transfer download path server-path-to-file
```

如果服务器为 TFTP 模式，还必须输入

```
transfer download tftpMaxRetries retries
transfer download tftpPktTimeout timeout
```

如果服务器为 FTP 模式，则需输入

```
transfer download username username
transfer download password password
transfer download port port
```

⑨ 输入 transfer download start 并采用 Y 回答，查看当前下载状态并开始下载进程。

⑩ 输入 Reset System 保存映像并重启系统。

⑪ 输入 config wlan enable *wlan_id* 重新使能 WLANs。

⑫ 输入 show sysinfo 查看系统版本是否升级成功。

6.2.3 使用 WCS 升级控制器软件

使用 WCS 升级控制器的软件，请按如下的步骤操作。

① 将最新的映像文件复制到 TFTP 服务器的根目录下，TFTP 服务器可以选择本地 WCS 自带的服务器，也可以选择外部 TFTP 服务器。

② 转到 Configure>Controllers，选择一个或多个 WLC，再从下拉命令列表中选择 download Software(tftp)或 FTP，如图 6-26 所示。

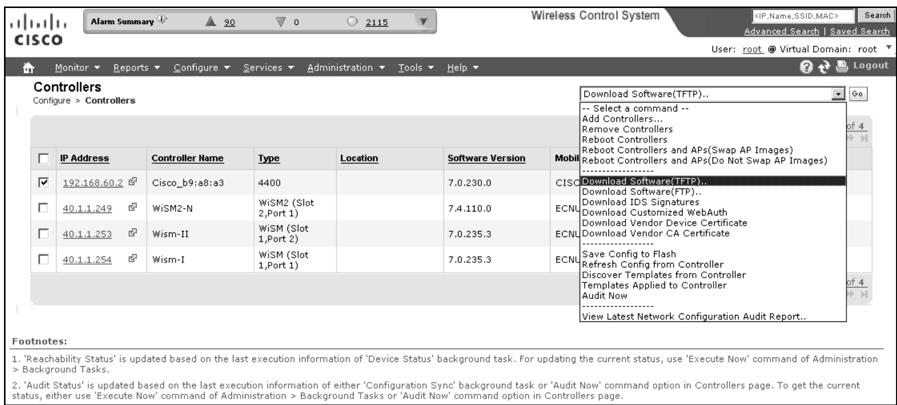


图 6-26 使用 WCS 下载文件到控制器

③ 配置合适的 TFTP 参数（此处不再重复），如图 6-27 所示。

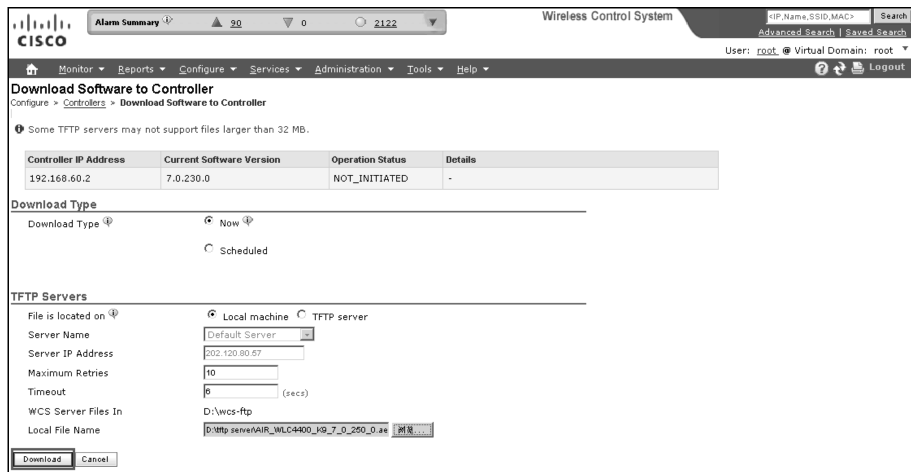


图 6-27　在 WCS 上配置 TFTP 服务器详细信息

④ 一旦映像文件被成功下载到控制器上，需要重新启动控制器以加载新的代码，在重新启动之前，先选择保存控制器的配置，如图 6-28 所示。

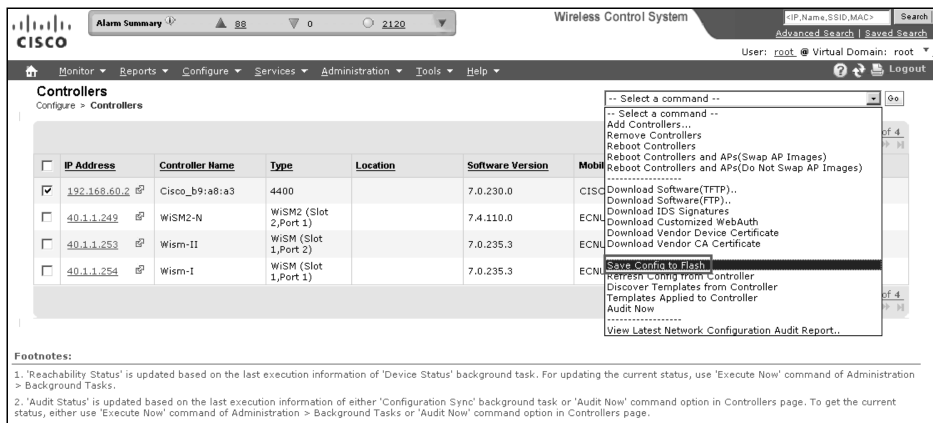


图 6-28　使用 WCS 保存控制器配置

⑤ 当保存完成后，再从命令列表中选择 Reboot Controllers，重新启动控制器，以便让新配置生效。

6.3　管理控制器配置文件

在升级控制器映像软件之前，Cisco 建议先上传控制器的配置文件，当控制器映像成功升级后，重新下载配置文件到控制器。

注意

4.2 版本之前的配置文件为二进制文件模式，4.2 之后的版本为 XML 模式，不要尝试更改 XML 格式的配置文件，否则将会导致 CRC 校验错误。

6.3.1 从控制器上传配置文件

可以采用 Web 方式或 CLI 方式完成此操作。

（1）采用 Web 方式上传配置文件

从 Web 界面上传配置文件，如图 6-29 所示。

① 选择 Commands > Upload File，打开上传文件配置窗口。

图 6-29 使用 WLC 的 Web 界面上传配置信息

② 从 File Type 下拉列表中选择 Configuration。

③ 如果需要对配置文件进行加密，则选中 Enable 左边的复选框，并在 Encryption Key 文本框中输入加密所用的密钥。

④ 选择 TFTP 或 FTP 的传输模式。

⑤ 输入 TFTP 或 FTP 服务器的 IP 地址、文件路径及存储的文件名，如果选择 FTP 模式，还需要输入 FTP 服务器的用户名、密码和端口号。

⑥ 单击 Upload 按钮将配置文件上传到服务器。

（2）使用 CLI 方式上传控制器的配置文件

① 登录到控制器的 CLI 界面。

② 输入 transfer upload mode {tftp | ftp}。

③ 输入 transfer upload datatype config。

④ 如果需要加密配置文件，则需要进行如下操作：

- 输入 transfer encrypt enable；
- 输入 transfer encrypt set-key key。

⑤ 输入服务器管理地址 transfer upload serverip *server-ip-address*。

⑥ 输入服务器的路径 transfer upload path *server-path-to-file*。

⑦ 输入需要保存的文件名 transfer upload filename *filename*。

⑧ 如果选择的是 FTP 的方式，还需要输入用户名、密码及端口号，采用如下的命令：

- transfer upload username *username*；
- transfer upload password *password*；
- transfer upload port *port*。

⑨ 输入 transfer upload start 查看当前上传的状态，如果正确，则输入 Y 开始上载进程。

```
Mode............................................. TFTP
TFTP Server IP.................................. 10.10.10.4
TFTP Path....................................... Config/
TFTP Filename.................................. AS_4402_4_2_55_8_Config.xml
Data Type....................................... Config File
Encryption...................................... Disabled
**************************************************
*** WARNING: Config File Encryption Disabled ***
**************************************************
Are you sure you want to start? (y/N) y
File transfer operation completed successfully
```

采用同样的方式可以将 TFTP 或 FTP 服务器上的配置文件下载到控制器上，此处不再赘述。

关于控制器的签名文件、CA 正书及厂商设备证书，可以采用同样方式下载到控制器上。

6.3.2　存储配置文件

控制器中包含易失性 RAM 和非易失性 NVRAM 2 种类型的 RAM。在任何时刻，我们都可以将配置文件从 RAM 存储到 NVRAM 中。以下的几种方式都可以保存机器的配置。

① 在 CLI 界面下，输入 save config 命令可以实时保存机器的配置。

② 当输入 reset system 后，系统将会要求用户保存当前配置并重新启动。

③ 当输入 logout 命令后，系统也会要求用户保存当前的配置。

利用 Web 方式，在右上角单击 Save Configuration 可以即时保存当前的配置，如图 6-30 所示。



图 6-30　使用 WLC 的 Web 界面保存配置信息

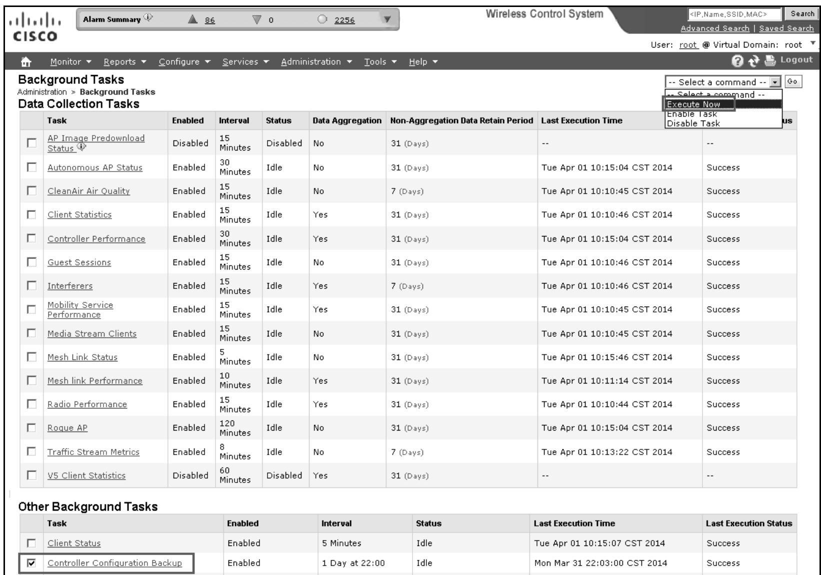
6.3.3　使用 WCS 管理控制器的配置文件

当 WLC 加入到 WCS 后，WLC 中完整的配置将从 WLC 中读出并在 WCS 的本地存储，当我们使用 WCS 更改 WLC 的配置时，WCS 将会自动更新 WLC 及本地的配置文件。如果在使用 WLC 的 Web 界面上更改 WLC 的配置，将会造成 WLC 本地和 WCS 上的配置不一致，此时可以刷新 WCS 上的配置。

转到 Configure >Controllers，选择需要刷新的一个或多个 WLC，从下拉列表中选择 Refresh Config from Controller，让 WCS 从 WLC 中重新加载配置文件到本地。

此时系统会要求用户选择保留还是删除 WCS 上的配置文件信息，通常选择 Retain，在控制器上保留原有的配置文件。选择确定，则系统将会刷新 WCS 本地配置文件并给出成功信息。

WCS 还可以定期在后台备份控制器的配置文件。选择 Administration>Background Tasks，在列表中选择 Controller Configuration Backup，再从列表中选择 Execute Now，就可以立即执行配置文件的备份，如图 6-31 所示。



Task	Enabled	Interval	Status	Data Aggregation	Non-Aggregation Data Retain Period	Last Execution Time	Last Execution Status
AP Image Predownload Status	Disabled	15 Minutes	Disabled	No	31 (Days)	--	--
Autonomous AP Status	Enabled	30 Minutes	Idle	No	31 (Days)	Tue Apr 01 10:15:04 CST 2014	Success
CleanAir Air Quality	Enabled	15 Minutes	Idle	No	7 (Days)	Tue Apr 01 10:10:45 CST 2014	Success
Client Statistics	Enabled	15 Minutes	Idle	Yes	31 (Days)	Tue Apr 01 10:10:46 CST 2014	Success
Controller Performance	Enabled	30 Minutes	Idle	Yes	31 (Days)	Tue Apr 01 10:15:04 CST 2014	Success
Guest Sessions	Enabled	15 Minutes	Idle	No	31 (Days)	Tue Apr 01 10:10:46 CST 2014	Success
Interferers	Enabled	15 Minutes	Idle	Yes	7 (Days)	Tue Apr 01 10:10:46 CST 2014	Success
Mobility Service Performance	Enabled	15 Minutes	Idle	Yes	31 (Days)	Tue Apr 01 10:10:45 CST 2014	Success
Media Stream Clients	Enabled	15 Minutes	Idle	No	31 (Days)	Tue Apr 01 10:10:45 CST 2014	Success
Mesh Link Status	Enabled	5 Minutes	Idle	No	31 (Days)	Tue Apr 01 10:15:46 CST 2014	Success
Mesh link Performance	Enabled	10 Minutes	Idle	Yes	31 (Days)	Tue Apr 01 10:11:14 CST 2014	Success
Radio Performance	Enabled	15 Minutes	Idle	Yes	31 (Days)	Tue Apr 01 10:10:44 CST 2014	Success
Rogue AP	Enabled	120 Minutes	Idle	No	31 (Days)	Tue Apr 01 10:15:04 CST 2014	Success
Traffic Stream Metrics	Enabled	8 Minutes	Idle	No	7 (Days)	Tue Apr 01 10:13:22 CST 2014	Success
V5 Client Statistics	Disabled	60 Minutes	Disabled	Yes	31 (Days)	--	--

Other Background Tasks

Task	Enabled	Interval	Status	Last Execution Time	Last Execution Status
Client Status	Enabled	5 Minutes	Idle	Tue Apr 01 10:15:07 CST 2014	Success
Controller Configuration Backup	Enabled	1 Day at 22:00	Idle	Mon Mar 31 22:03:00 CST 2014	Success

图 6-31　使用 WCS 备份控制器的配置文件

通过此窗口还可以更改备份的每天执行时间。

6.4　清除控制器配置文件

6.4.1　采用 CLI 方式

① 在命令行下输入 clear config，并输入 Y 确认。
② 输入 reset system，并输入 N 确认不需要保存配置文件就重新启动系统。
③ 系统重新启动后将会重新进入初始配置界面。

6.4.2　采用 Web 方式

在 Web 界面上，单击 COMMANDS>Reset to Factory Default>Reset，系统弹出“是否确认将配置文件恢复到出厂设置”，单击“确认”按钮后，重新启动系统，控制器将恢复到出厂设置状态，如图 6-32 所示。



图 6-32　使用 WLC 的 Web 界面将 WLC 恢复出厂设置

6.4.3　采用 WCS 方式

在 WCS 界面中，选择 Configure>controllers>192.168.60.2>System>Commands，再从右侧的 Administrative Commands 的下拉列表中选择 Reset to Factory Default，单击 GO 既可以将控制器恢复到出厂状态，如图 6-33 所示。

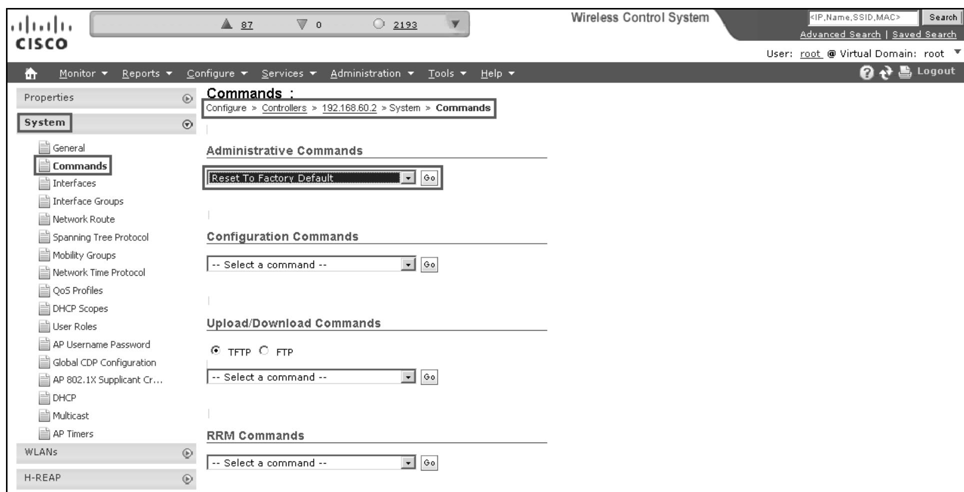


图 6-33　使用 WCS 恢复 WLC 的出厂设置

6.4.4　删除控制器配置

删除控制器配置信息只能通过控制台端口完成，通常发生在用户遗忘超级管理员密码的场合或者需要对控制器进行全新配置的场合。

在控制台窗口下，输入 Reset System，在系统弹出是否需要保存配置时，输入 Y 确认，重新启动系统；如果忘记超级用户密码，则使用电源按钮重新启动系统。

当系统重启完成后，要求用户输入管理用户名时，输入 recover-config，将会把控制器恢复到出厂状态。

接下来就可以重新配置控制器，具体配置过程如前面章节所述。

6.5　重新启动控制器

当重新启动控制器时，可以通过 CLI 端口观察控制器启动时的状态。

6.5.1　通过 Web 方式重新启动

在 Web 界面上，选择 Commands>System Reboot，单击 Reboot 按钮，如图 6-34 所示。

如果没有保存配置，则系统要求用户在保存配置后立即重新启动。

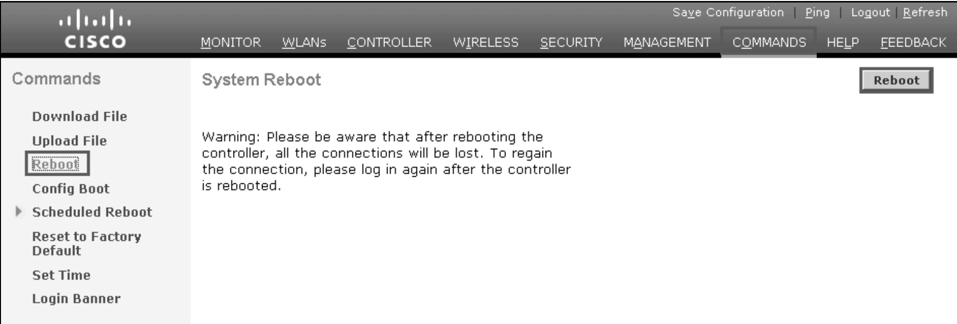


图 6-34　使用 WLC 的 Web 界面重新启动 WLC

6.5.2　通过 WCS 方式重新启动

在 WCS 中选择 Configure>Controllers，选择需要重新启动的一台或多台控制器，从下拉命令菜单中选择 Reboot Controllers，便可以重新启动控制器，如图 6-35 所示。

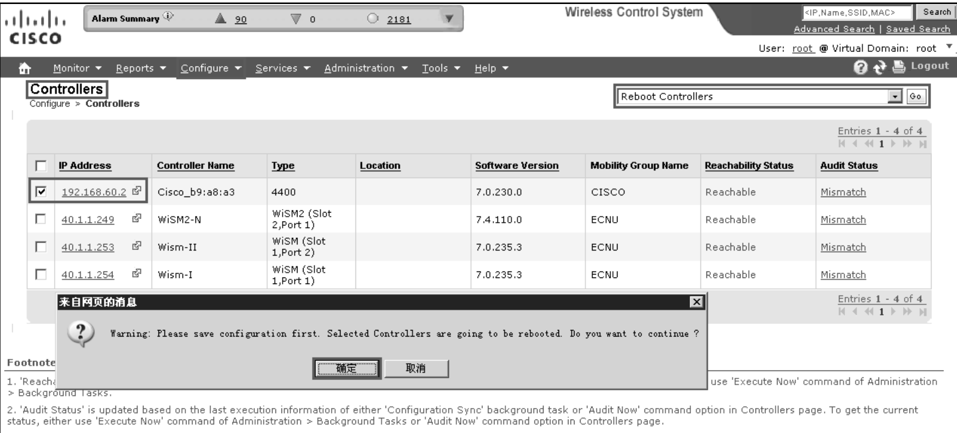


图 6-35　使用 WCS 重新启动 WLC

6.5.3　通过 CLI 方式启动

在控制台窗口下，输入 Reset System，在系统弹出是否需要保存配置时，输入 Y 确认，重新启动系统。

在系统重新启动后，将会显示如下的自检信息：

① 初始化系统。

② 检测硬件的配置。

③ 将微代码加载进入内存。

④ 检测操作系统软件是否加载。

⑤ 初始化保存的配置文件。

⑥ 显示登录窗口。

当忘记密码或系统宕机时，可以采用直接开关电源的方式启动系统，但此方式可能会造成配置丢失，建议不要使用。

第7章



无线现场勘察

本章要点

- 无线勘察概述及前期准备
- 无线勘查的现场工作
- 勘察后需验证的重点项目
- 无线网络的性能优化

无线局域网部署的第一个步骤就是现场勘察，以评估在特定环境中 RF 的传输行为，如果无线网络在部署前计划不周或现场勘查不完备，在实际运行过程中可能会出现很多问题，本章将讲述无线现场勘察的相关知识。

7.1 无线勘察概述及前期准备

为了实施现场勘查工作，我们应该具备如下的知识：

- IEEE 802.11 无线的基本知识；
- 无线局域网规划的相关知识。

7.1.1 无线勘察的种类

无线现场勘察有如下三种类型。

（1）被动勘察

被动勘察只使用监听模式进行，用来进行勘察的无线客户端无须同无线接入点进行关联。当希望查找欺诈设备或想获得无线发射设备的下行射频覆盖范围时，可以采用这种勘察方式。使用被动勘察可以确定欺诈的无线接入设备，可以快速查找射频问题区域，可以对射频的设置进行验证。被动勘察最显著的不足是缺失了上行链路信息、物理层（PHY）数据传输速率和重传等信息。物理层数据传输速率一般根据射频信号和噪声水平建立，被动勘察报告得出的射频参数同物理层实际数据传输速率存在较大的差异，因此被动勘查一般只用于初步的勘察，而且仅能得到与信标帧相关的信号信息。

（2）主动勘察

主动勘察在整个勘察的过程中使用关联到无线接入点的客户端进行，当客户端同 AP 建立关联后，它即可以执行一个典型 IEEE 802.11 客户端能够执行的所有任务，其中包括根据射频条件的变化调整数据传输速率并进行重传。主动勘察通常用于新的 WLAN 部署，它可以提供大部分的细节并以此为基础设计无线网络。

主动勘察主要使用以下两种方法。

- 基于 BSSID：此方法将无线客户端锁定到一个无线接入点的射频接口 MAC 地址并防止客户端在相同 SSID 的 AP 间进行漫游。
- 基于服务集标识符（SSID）：这是较为常用的部署后的场景，用来勘察多个无线接入点，它将勘察客户端关联到一个 SSID 且允许客户端在多个无线接入点之间漫游。

（3）预测勘察

预测勘察通过软件程序进行，该程序基于射频算法使用覆盖面积信息来执行无线接入点的部署预测，这种勘察通常不进行任何类型的现场测量。预测勘察一般在部署环境尚未建成时进行，目的是为了获得与 WLAN 部署相关的硬件预算。

7.1.2　无线勘察的前期准备

在进行无线现场勘察前，须做好如下的前期工作。

① 了解射频的应用需求：仅用于数据，还是有语音、定位等方面的需求？

② 了解建筑物的类型：内部是混凝土墙壁还是石膏板隔墙？是在某楼层进行无线覆盖还是多个楼层甚至整幢楼进行覆盖？是否要包含室外区域？是否有仓库等特殊的区域？

③ 列举用户可能使用的不同类型的上网设备：包括是否含有 IEEE 802.11b 的上网设备？无线终端设备所能接受的最小接收信号强度指示（RSSI）是多少？最小信噪比（SNR）是多少？时延和抖动容忍度如何？最大发射功率是多少？

获取以上的需求后，即可以对照楼层数字平面图进入建筑物内部进行造访，认真确定建筑物的类型，确认勘察的区域，标注最困难的覆盖区域，检查主要覆盖区域在楼层平面图上没有提到的细节，检查哪些可能存在漫游的地点。根据建筑物及用户需求的具体情况决定是否采用高密度接入部署，是否对 AP 的发射天线有特殊的需求？如果安全性较高，为防止非法 AP，考虑是否需要放置额外的监视和嗅探模式无线接入点，是否需要部署专用的定位 AP？如果要安装室外 AP，还需要做好防雷和接地工作。

接下来可以采用专业勘察工具，如 AirMagnet 公司或 Ekahau 公司的现场勘察工具，进行无线现场勘察。

7.1.3　现场勘察事项的基本清单核对

① 确定要使用的频段：2.4 GHz 还是 5 GHz。

② 勘察工具软件的选择：AirMagnet 或 Ekahau。

③ 采用的勘察模式：是主动勘察还是被动勘察。

④ 选择被用来执行勘察的无线适配器。

⑤ 覆盖区域的确定：如楼梯间、电梯、配电房、通风井、机械区域等是否需要覆盖。

⑥ 热图显示射频覆盖区域的蜂窝边缘均满足目标 RSSI，热图显示覆盖区域的信噪比均满足目标信噪比，热图显示覆盖区域的噪声级别满足目标级别。

⑦ 确定并列出可能的干扰源：在整个建筑设施中寻找可能的干扰源，如微波炉、无绳电话等。

⑧ 实际将要安装的无线接入点硬件类型：Aironet 3500 系列无线接入点的热图与 Aireonet 3600 系列无线接入点的热图是不同的，勘察时应选择计划购买并实际部署的无线接入点类型进行现场勘察。

⑨ 确定勘察的应用类型：语音、定位，还是只有数据。

7.2 无线勘查的现场工作

7.2.1 地图的校准

在勘察工具中校准地图允许你定义地图上两点之间的正确距离。例如，你可以在地图中一面 40 英尺长的墙上画一条线并指定该线代表 40 英尺的距离。其余的地图可以基于该线定义的距离重新调整。

如果地图不正确校准，无线接入点产生的热图将不代表正确的距离。从不正确校准的地图勘察报告收集的数据结果将无法使用。如果勘察报告中的热图看起来不正确，建议校准验证地图，校准的最佳实践是查看无线接入点热图覆盖范围看起来是否过大或过小，大多数情况下，当在地图上看到一个数据点或无线接入点的射频覆盖相比实际覆盖更大时，就需要校准地图。例如，你可能会看到一个无线接入点的热图就覆盖了整个楼层，这可能是校准不正确引起的后果。

可能还要注意到，地图看起来不准确，图像发生了拉伸或扭曲。这表示地图是没有被正确缩放，如图 7-1 所示。最佳实践是，当你在地图上测量距离时应该使用较长的距离，这样校准的结果往往更准确。

注意

勘察后就不能重新校准地图，也不能修复地图校准时所采取的不正确缩放产生的勘察数据，必须更正地图校准并重新执行勘察。

在勘察时应该总是验证地图校准，方法就是在地图上测量两点之间的距离，并在实际中验证准确性。可以使用 AirMagnet Survey 的“测量工具”来衡量所需地图上的点之间的距离。

正确校准后的地图如图 7-2 所示，测量工具如图 7.3 所示。

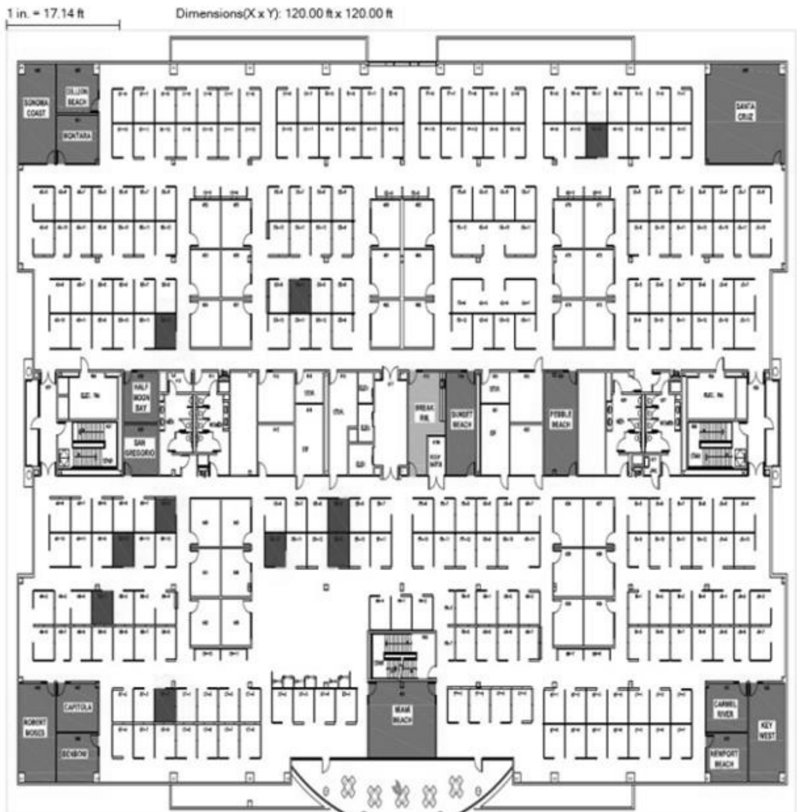


图 7-1　不当缩放地图，地图尺寸为 120 英尺×120 英尺

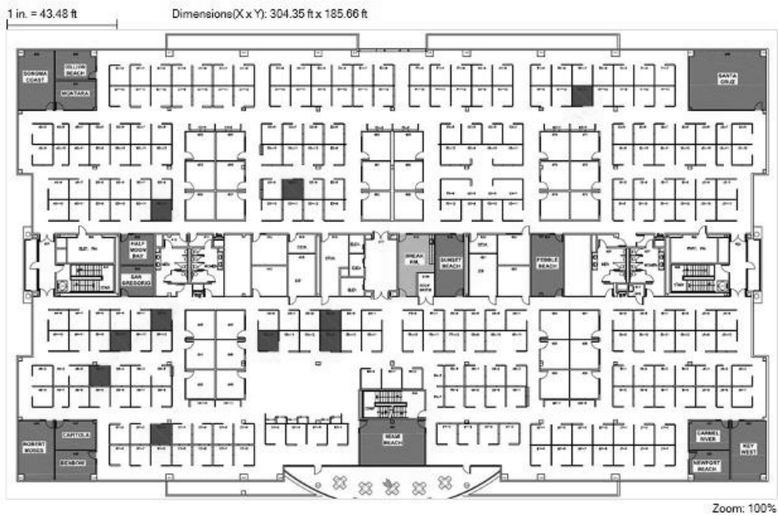


图 7-2　正确校准后的地图

7.2.2 信号的传播

“信号传播评估”允许现场勘查中的应用程序预测数据点之间的信号传播，如果该值太高，则测试结果可能不准确，即在覆盖范围不足的地方也有可能会显示可接受的信号电平。如果一份报告中的无线信号可以穿透大楼墙壁到达很远处，那可能是一个“信号传播评估”设置过高的迹象。AirMagnet 的默认值是 40 英尺，这在实际中可能并不是特别精确，如果设定为 15～20 英尺则可以提供更准确的结果。正如前面提到的，最好的做法是每一次都仔细查看无线接入点热图，关注每个无线接入点的信号可以传多远，同时也应该注意到，当远离无线接入点时，信号会逐渐变弱。在完成勘察后，可以改变信号的传播评估值，而无须再次进行勘察。更改信号传播的默认值示意图如图 7-4 所示。



图 7-3　测量工具

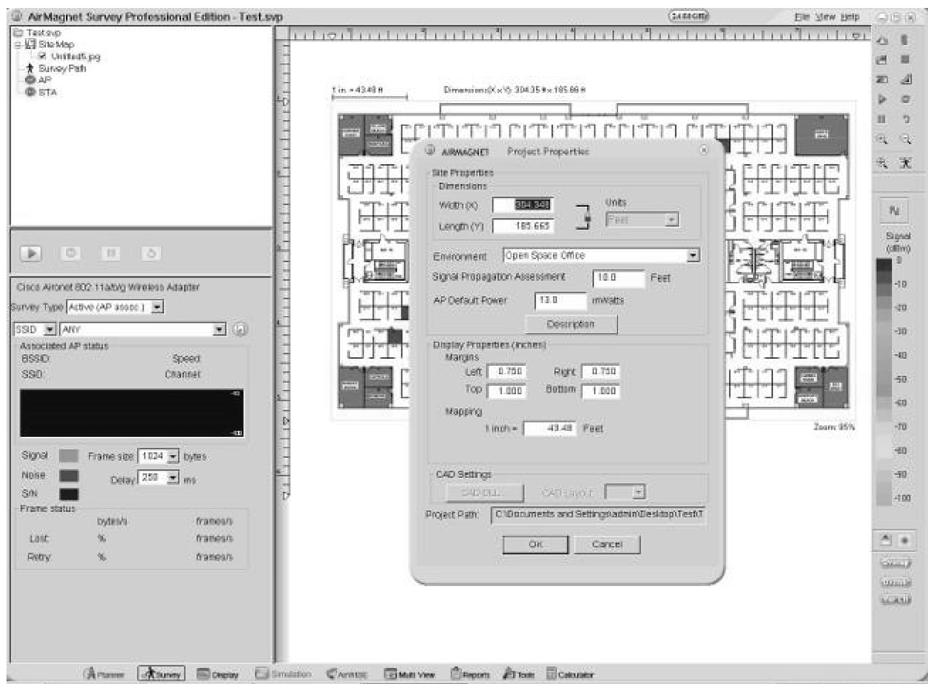


图 7-4　更改信号传播的默认值示意图

7.2.3 勘察路线

验证勘察路径上的数据收集点是很重要的，勘察路径应遵循有效行走的路径，不应该选择让路径穿过墙壁，勘察路径应该包含一些在需要无线覆盖的房间中的数据收集点，有些办公室

虽然没有数据收集点，但是仍然可能会被无线所覆盖，在室内勘察时，最好保证办公室的门在被收集数据的时候处于关闭状态。

1．不完整的步行路线（如图 7-5 所示）

并不是在所有的地点都拥有数据勘察点，例如，在办公室内部平面图底部的区域，白色区域表示没有测量收集数据的地点。

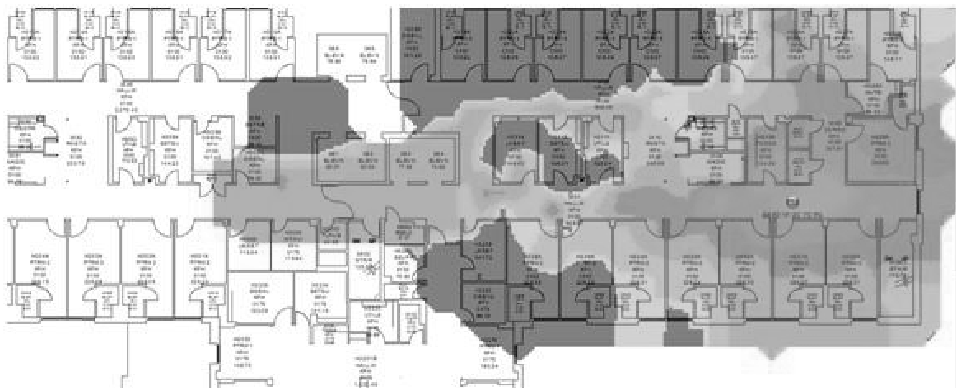


图 7-5　不完整的步行勘察路径

2．完整的步行路线（如图 7-6 所示）

数据点可在办公室内沿着底部的楼层规划平面布局图被采集，这些可通过在房间内部的实线和虚线来显示。

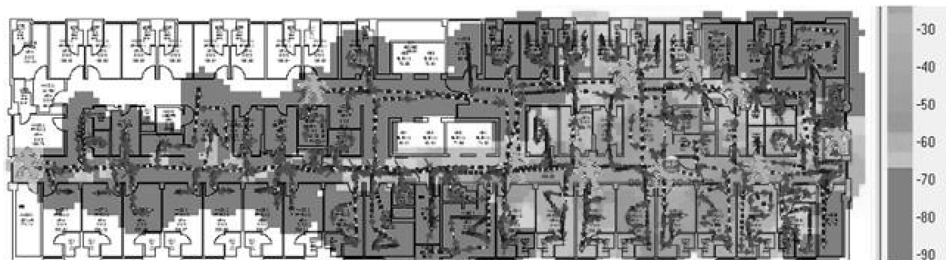


图 7-6　完整的步行勘察路径

对于像会议室可能会有高密度客户端接入的区域，在考虑覆盖的同时，考虑客户端的密度也非常重要。当考虑客户端数量时，需要弄清哪些应用程序会在客户端设备上使用，这样可以帮助了解客户端总共需要多少带宽。

7.2.4 信道扫描

仔细检查“信道扫描列表”以确保目前正在使用的信道已经存在于其中，强烈建议只扫描那些无线 AP 正在使用的信道。如果勘察时在数据点之间走得太快，将不能提供足够的时间让无线适配器完成整个信道扫描，导致不准确的结果。如果需要扫描恶意无线发射设备，过快的行走速度可能会使那些恶意设备无法出现在扫描列表上。信道扫描列表如图 7-7 所示。

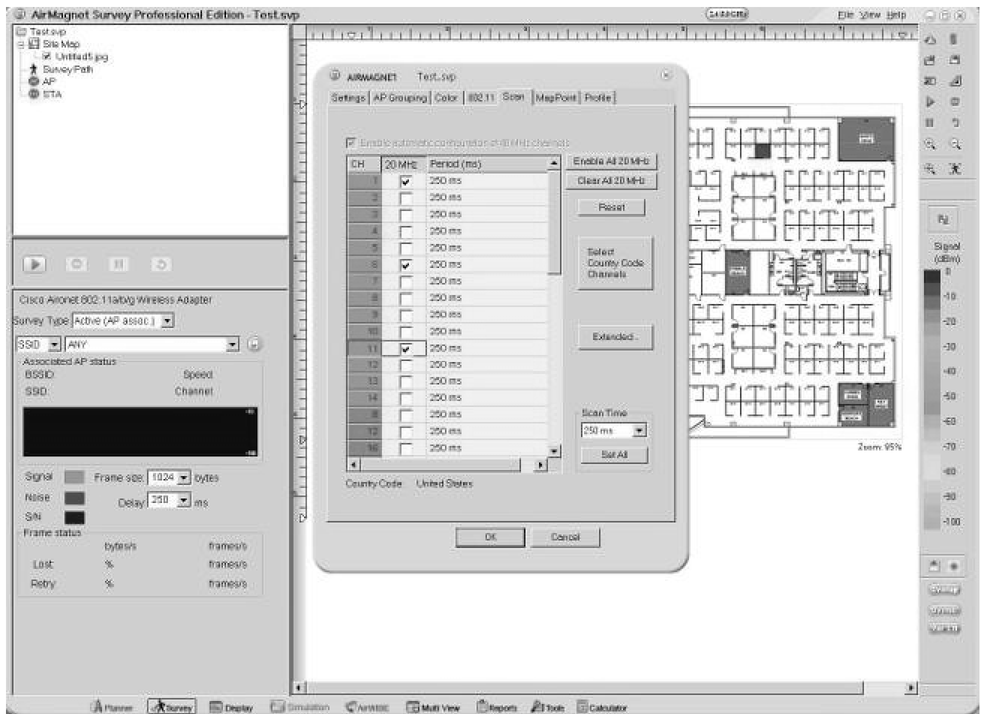


图 7-7 信道扫描列表

另一项建议是只扫描或查看无线 AP 所使用到的 SSID 的热图，当建筑中有属于其他公司的楼层时要格外注意，不要误将其他公司的无线射频当作当前业主的热图。在进行现场勘查时一定要选择使用恰当的无线网络适配器，适配器的选择要同实际使用的适配器拥有相同或相似的特征，如果使用较高接收灵敏度以及更高增益的天线所得出的结论同实际中使用的无线适配器相比将不具有任何可比性。

7.3 勘察后需验证的重点项目

现场勘察后进行验证的首要目的是提供关于当前射频覆盖范围的详细资料，并确定是否有足够的覆盖以支持网络最初设计的要求。验证的目的还应该提供包括定位干扰源设备、欺诈设

备的位置等信息，经过验证的现场勘察文件将作为无线 AP 部署的指南。

7.3.1　覆盖

覆盖范围是无线客户端为克服射频干扰关联到一个无线接入点的所需信号强度、质量的表征。一个无线接入点覆盖范围的边缘是通过将客户端设备逐渐远离无线接入点时基于信号强度和信噪比来测量的，覆盖所需的信号的强弱依赖于特定类型的客户端设备以及网络上的应用。

为了支持无线语音 IP 电话（VoIP）要求，请参阅思科 7925G 无线 IP 电话部署指南中指定的射频指引，思科推荐的最小语音应用的无线信号强度为–67 dBm，最小信噪比为 25 dB。

后现场勘察分析的第一步是验证“信号覆盖”，信号覆盖的测量单位是 dBm，可以通过调整颜色编码来选择所允许的最小信号电平，用以查看覆盖是否满足要求。图 7-8 中的示例显示蓝色、绿色、黄色区域信号覆盖范围内信号强度为–67 dBm 或更好，图中有色区域表示覆盖不完善。

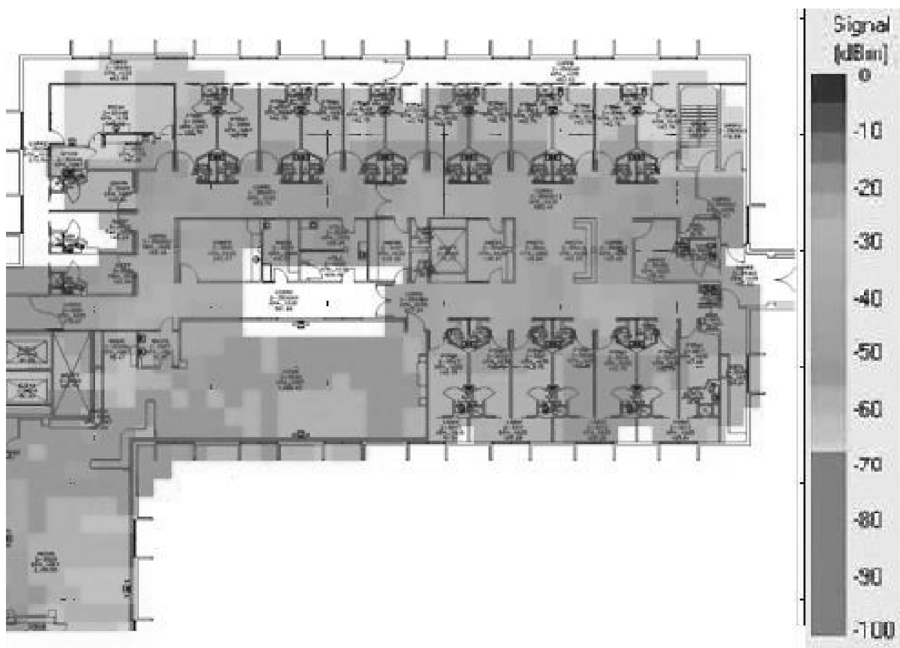


图 7-8　–67 dBm 时的信号覆盖

当检查信号覆盖范围时，要确保无线接入点的无线电发射功率不超过客户端设备可以支持的功率。例如，默认情况下，思科无线 IP 电话 7925G 可以使用的最高发射功率（默认情况下，2.4 GHz 为 17 dBm/50 mW；5 GHz 为 16 dBm/40 mW）。即使调查报告中的所有区域中都有很好的覆盖效果，但如果无线接入点使用最高发射功率传输数据，而客户端设备不支持如此高的

发射功率时，可能产生数据上行的问题。对于缺乏覆盖的地区，可以通过增加无线接入点的发射功率来扩大覆盖，但如果对应的客户端设备不支持，那么此时只能提高下行链路的覆盖范围，而无法成功进行双向数据沟通。

无线接入点与客户端发射功率对比如图 7-9 所示。

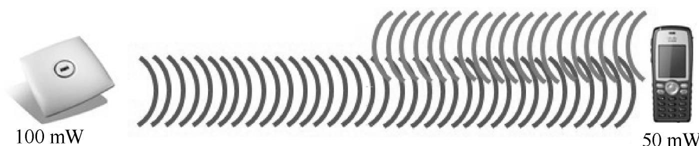


图 7-9　无线接入点与客户端发射功率对比

7.3.2　信道重叠

通过现场勘察检验并确定设备在成功漫游到下一个无线接入点之前，信号是否会从前一个关联的无线接入点丢失。例如，基于《思科 7925G 无线 IP 电话部署指南》中指定的射频指导方针，当手持无线 IP 话机被部署在 IEEE 802.11b/g 的环境中时，必须使用非重叠的信道并允许至少有 20%的相邻信道重叠。对于语音部署，推荐的功率值为蜂窝边缘–67 dBm，信道之间有 20%的重叠。

信道重叠如图 7-10 所示。

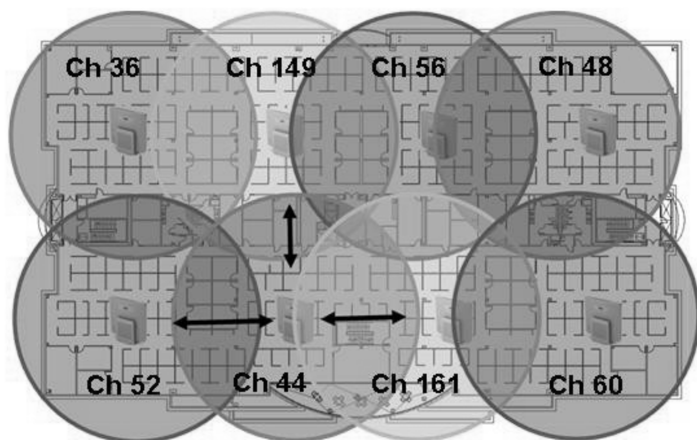


图 7-10　信道重叠

7.3.3　信号噪声比

SNR 是传输信号在指定信道上与背景噪声的比值。思科 7925G 无线 IP 电话部署指南中要求最小信噪比是 25 dB（25 dB 相当于在–67 dBm 的信号强度情况下，仅有–92 dBm 的噪声级

别）。可以在 AirMagnet 的工具栏上查看 SNR 的热图，同时通过下拉菜单来改变选择信号覆盖的信噪比。还可以通过调整颜色编码来显示所允许的最低信噪比水平，在图 7-11 所示的映射图中，蓝色、绿色、黄色区域具有 25 dB 或更好的信噪比（SNR），灰色的区域则表示该区域不能满足最低信噪比 25 dB 的要求。

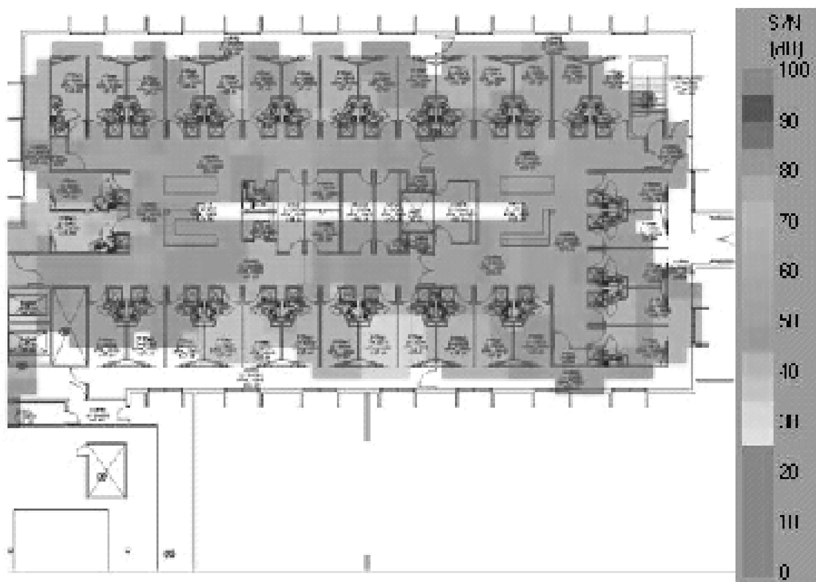


图 7-11　在 25 dB 的时信噪比

7.3.4　本底噪声

本底噪声混合了系统自身和周围环境中存在的所有背景射频，射频信号的强度必须要超越本底噪声的大小，才能被接收器识别成为一个有效且有用的信号。对于一个信噪比为 25 dB 且信号噪声级别在–67 dBm 的信号来说，信号的噪声级别不得超过–92 dBm。在 AirMagnet 的工具栏上，可以查看“本底噪声”的热图，并且在下拉菜单中可以选择更改为本底噪声。

在本底噪声电平超过–92 dBm 的地方，还可以通过调整颜色编码表示来显示最小允许的噪声本底水平。如图 7-12 中所示的深灰色地带的噪音水平不超过–92 dBm。浅灰色区域的噪声水平超过了–92 dBm。

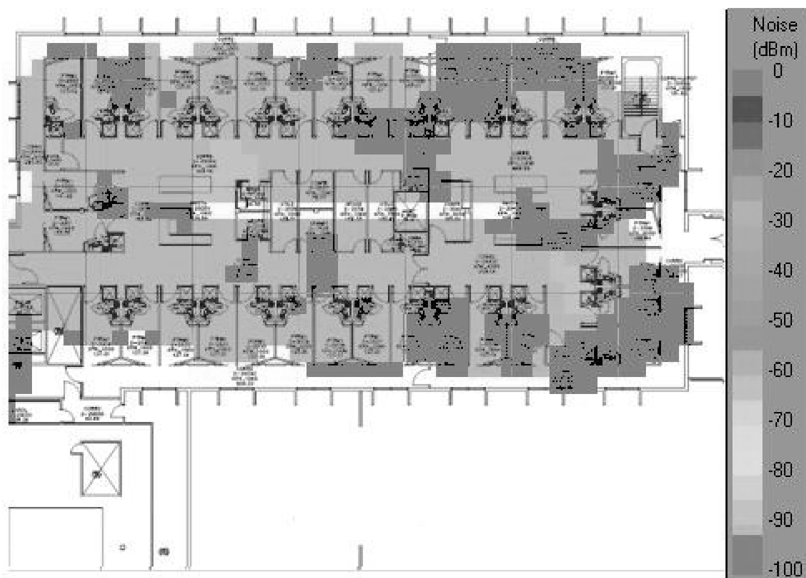


图 7-12　本底噪声为–92 dBm

7.3.5　信号泄露和非法设备射频干扰

射频信号可以在楼上、楼下之间泄露，穿透地板的射频信号量可能会导致同信道干扰，为此，一般需要降低无线接入点的射频发射功率。通过查看每一层楼的无线接入点布置图可以确定是否有无线接入点被放置在上下的重叠位置。总的来说，在楼层之间部署的 AP 应相互错开，以提供更好的覆盖率。查看无线接入点无线电邻居列表可用来验证泄露问题，同时也可以用来验证不同楼层之间的无线接入点是否拥有很强的发射功率。思科支持社区提供思科无线控制器配置分析工具，该工具可以提供相邻无线接入点的详细信息。

非法无线接入点是指未经企业信息技术部门授权而安装的无线接入点，大多数非法无线接入点缺乏安全保证，可能被外人用来接入企业网络。除了非法设备所带来的安全风险，它们更会导致同信道和相邻信道的射频干扰，从而降低企业无线局域网的性能。如果这些无线接入点没有业务接入的理由，应该立即断开它们与企业网的连接。一旦关闭了这些无线接入点的连接，会对网络的整体安全性提升和降低射频干扰方面有很大的帮助。但如果这些无线接入点正在为业务服务，应该勘察这些服务并让其成为当前企业无线局域网基础设施的一部分。

通常需要通过思科频谱专家（Spectrum Experts）来进行一次单独的路径检测，通过检测可以查出非法设备和接口，并且可以通过快照的方式展现出来。

思科频谱专家如图 7-13 所示。

Spectrum AQ | Spectrum (2) Spec An | Devices | Channel Summary | Device Finder

Devices: Last 10 Minutes, All Channels

Device	Signal Strength (dBm)	Duty Cycle (%)	Discovery Time	On Time	Channels Affected	Network ID	Device ID
lyndas network (Ch 11)	-96.0		Mon May 18 12:4...	00:01:43 (Down)	None	00:19:E3:FA:AC:C4	00:19:E3:FA:AC:C4
linksys_SES_3152 (Ch 6)	-93.0		Mon May 18 12:4...	00:02:02 (Down)	None	00:13:10:FE:92:C2	00:13:10:FE:92:C2
linksys_SES_3152 (Ch 6)	-95.0		Mon May 18 12:4...	00:00:18 (Down)	None	00:13:10:FE:92:C2	00:13:10:FE:92:C2
linksys (Ch 6)	-92.0		Mon May 18 12:4...	00:00:30	5..7	00:1C:10:93:82:EF	00:1C:10:93:82:EF
linksys (Ch 6)	-95.0		Mon May 18 12:4...	00:01:43 (Down)	None	00:1C:10:93:82:EF	00:1C:10:93:82:EF
linksys (Ch 6)	-87.0		Mon May 18 12:4...	00:03:30	5..7	00:16:B6:08:B2:8E	00:16:B6:08:B2:8E
Johnswireless (Ch 4)	-96.0		Mon May 18 12:4...	00:03:30	None	00:06:B1:14:01:2B	00:06:B1:14:01:2B
freedom (Ch 6)	-91.0		Mon May 18 12:4...	00:03:30	5..7	00:23:97:05:E1:71	00:23:97:05:E1:71
Dynex (Ch 11)	-90.0		Mon May 18 12:4...	00:02:01 (Down)	10..12	00:1C:DF:0E:2C:EC	00:1C:DF:0E:2C:EC
default (Ch 6)	-92.0		Mon May 18 12:4...	00:01:14 (Down)	5..7	00:11:95:4C:D1:23	00:11:95:4C:D1:23
COVESIDE NETGEAR (Ch 11)	-98.0		Mon May 18 12:4...	00:00:37 (Down)	None	00:18:4D:8B:94:D4	00:18:4D:8B:94:D4
Belkin_N1_Wireless_A48C93...	-86.0		Mon May 18 12:4...	00:03:30	4..8	00:1C:DF:A4:8C:93	00:1C:DF:A4:8C:93
Beacon Wi-Fi Network AP 1 (...	-93.0		Mon May 18 12:4...	00:03:30	1..2	00:03:52:A2:61:40	00:03:52:A2:61:40
Beacon Wi-Fi Network (Ch 1)	-92.0		Mon May 18 12:4...	00:03:00	None	00:02:2D:8B:70:2E	00:02:2D:8B:70:2E
Beacon Wi-Fi Network (Ch 1)	-94.0		Mon May 18 12:4...	00:00:27 (Down)	None	00:02:2D:8B:70:2E	00:02:2D:8B:70:2E
Apple Network 0988dd (Ch 6)	-91.0		Mon May 18 12:4...	00:03:30	None	00:1F:F3:09:88:DD	00:1F:F3:09:88:DD
07FX10055314 (Ch 6)	-95.0		Mon May 18 12:4...	00:00:45	None	00:12:0E:8D:A9:29	00:12:0E:8D:A9:29
⊟ Cordless Phones [1]							
DECT-Like Base Station 1	-80.8	2	Mon May 18 12:4...	00:00:43 (Down)	1..5;8..13	C2:60:98:CB:19	

图 7-13　思科频谱专家

不能只依赖报告或基础设施来检测和报告非法设备和干扰源，通过基础设施设备检测出的非法设备应当上报管理系统做进一步分流和调查。

7.3.6　使用无线控制器的链路测试功能协助评估覆盖

为了确定当前无线接入点的覆盖在客户端上运行应用程序是否足够，无线控制器提供给客户一个用户友好的链路测试工具。

步骤 1：对于关联到无线接入点的客户端，可以通过 MAC 地址来进行匹配，选择 WLC >Monitor>Clients，客户端链路测试选项如图 7-14 所示。

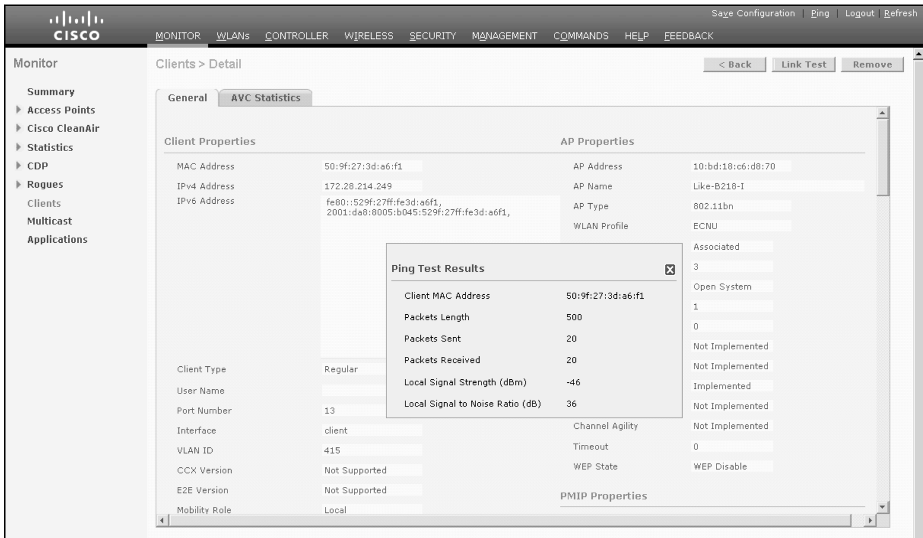


图 7-14　客户端链路测试选项

步骤 2：单击“Link Test”按钮，运行链路测试程序。此操作将执行一个双向链路测试，确定当前客户端的覆盖情况。如果没有丢失的数据包，那么下一步尝试将客户端远离无线接入点，以确定是否在任意可用的有效范围内都可以保证应用程序性能。

7.4 无线网络的性能优化

7.4.1 无线数据传输速率

无线数据速率配置工具是调节和优化无线网络中最关键的工具之一，数据传输速率的选择直接影响无线的覆盖范围和性能，因此，了解数据传输速率变化对环境的影响非常重要。无线数据传输处于低速率时会比高速率传输得更远，通过降低数据的传输速率可以增加无线接入点的有效覆盖范围，通过禁用无线接入点的低传输速率，可以减少无线接入点的有效覆盖范围。

如图 7-15 所示，如果增加覆盖范围，将会降低连接速度，从而降低整个系统的吞吐量。在 2.4 GHz 的部署中，因只有三个互不重叠的信道，增大覆盖范围可能会出现相同信道的干扰，如图 7-16 所示。相反，如果减小覆盖的范围，将会提升整体性能并能够减少同信道的干扰，有效降低信道使用率。

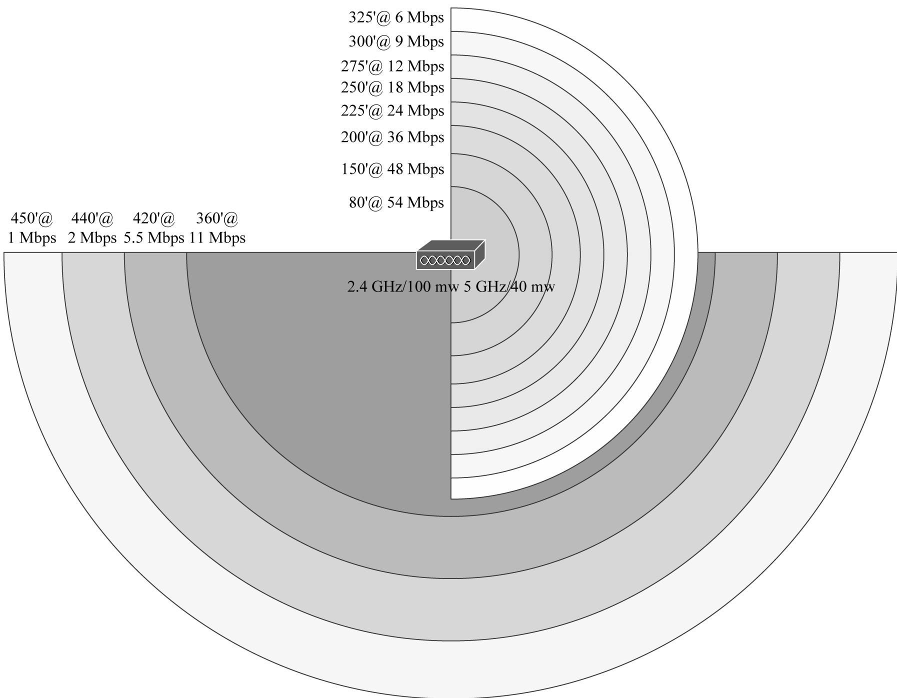


图 7-15　无线覆盖（蜂窝大小）（一）

为平衡这些选项以实现最佳的性能，关键是要在无线接入点的密度和客户端 / 应用程序的需求之间进行折中选择。例如，如果需要提供无线语音服务，那么就提高 AP 部署的密度并通过禁用较低的传输数据速率来增强无线接入点的性能（思科 792x 系列 WiFi 电话需要最低数据率为 12 Mbps）。如果在仓库中使用的是传统的 IEEE 802.11b 扫描终端，那么必须保持低速率的启用。无线控制器 7.2 版以上的软件通过使用射频配置文件增强了对环境的控制，它允许基于每一个 AP Group 设置数据传输速率。一般情况下，多数无线部署都会启用最低速率作为其强制速率，高密度部署和组播部署环境可能会有多个较高强制速率。

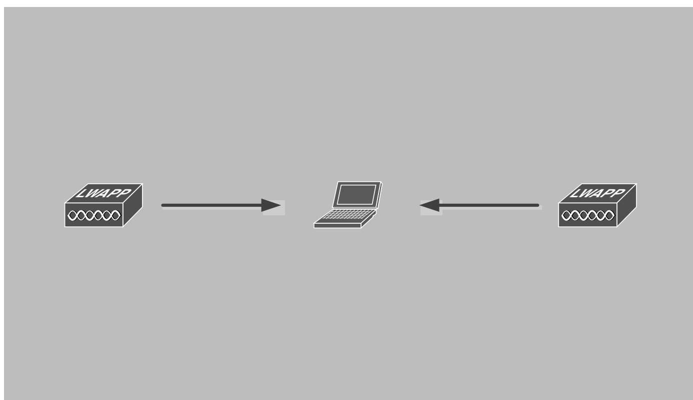


图 7-16　无线覆盖（蜂窝大小）（二）

7.4.2　管理帧

IEEE 802.11 管理帧以强制性的最低（基本）数据传输速率传输，最需要关注的问题是信标帧流量。例如，在一个 WLAN 密集部署的环境中存在 6 个不同的 SSID，1 Mbps 被定义为强制速率，那么将会有 67.2%的时间（Airtime）被信标所使用。如果最低的强制速率是 12 Mbps，则只有百分之五的时间会被信标消耗。如果禁用较低的强制速率同时对 SSID 的数量进行限制，可以减少管理帧花费的带宽，为连接的客户端提供更多的带宽。

当强制速率为 1 Mbps 时，如果信标帧的平均长度为 140 字节，时间间隔为 100 ms，周围存在 10 个 AP，每个 AP 上有 6 个不同的 SSID，则信标帧占用的时间率计算如下：

$$\frac{140\times8\times6\times10}{1\times10^6}=67.2\text{ ms}$$

$$67.2/100=67.2\%$$

如果其他条件相同，强制速率为 54 Mbps，则信标帧占用的时间率为：

$$\frac{140\times8\times6\times10}{54\times10^6}=1.244\text{ ms}$$

$$1.244/100=1.244\%$$

管理帧占用带宽示例如图 7-17 所示。

Network Configuration	Value
Average Beacon Size (bytes)	140
Beacon Interval (ms)	100
Number of SSIDs per AP	6
Number of Nearby APs	10

Results	bps
Beacon Utilization	672,000

Basic Data Rate	Bandwith Utilization
1 Mbps	67.20%
2 Mbps	33.60%
5.5 Mbps	12.22%
6 Mbps	11.20%
9 Mbps	7.47%
11 Mbps	6.11%
12 Mbps	5.60%
18 Mbps	3.73%
24 Mbps	2.80%
36 Mbps	1.40%
48 Mbps	1.87%
54 Mbps	1.24%

图 7-17　管理帧占用带宽示例

7.4.3　组播数据的传输

一般情况下，组播 / 广播帧会以最高强制速率发送，例外情况就是在当前同 AP 关联客户端中有使用比最高强制速率更低速率进行关联时，无线接入点将使用比当前所有的客户端连接速率都要低的强制速率发送。例如，将最高强制速率设定为 24 Mbps，而将最低强制速率设置为 6 Mbps，如果在 BSSID 上的所有客户端都使用 24 Mbps 或更高的传输速率，则使用 24 Mbps 来传输组播。但是，如果任何一个客户端的速率下降到 6 Mbps，那么组播传输将会使用 6 Mbps。否则，低速客户端将无法接收组播报文。

通过更改强制速率可以提升组播性能，当设置较高的强制速率时，将使组播流的传递拥有更高的带宽，尽管可能会造成某些客户端无法可靠地接收数据流。如果设置了较低的强制速率，这虽然使得低速客户端可以接收到组播，但是以牺牲整个无线的性能为代价的。

附录A



Cisco 自主 AP 和轻量级 AP 之间的转换

本章要点

- 升级前的准备
- 升级过程
- 安装并运行升级工具必须满足的要求
- 安装并运行升级软件 Upgrade Tool
- IEEE 802.11n AP 的升级

A.1 升级前的准备

① 调整好网络结构，以使升级的 AP 能够自动发现控制器 WLC。
② 自主 AP 必须运行 IOS 12.3（7）JA 及以上的版本，如果版本太低，必须先升级版本。
③ 配置好控制器以便升级时使用。
④ 下载升级工具：http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless。
⑤ 准备网络架构。
⑥ 配置好控制器以便升级时使用。
⑦ 将控制器的主版本升级到 3.1 级以后。
⑧ 在控制器上允许 Telnet 连接。
⑨ 使升级客户端计算机的时间与控制器的时间同步。

在控制器上，允许 Telnet 连接通过命令行或 Web 管理页面进行。当通过命令行进行时，输入命令 config network telnet enable；当通过 Web 管理页面进行时，通过 Web 界面打开 Telnet，在登录后，选择 management 的链接，然后依次选择 Telnet-SSH、Allow New Telnet Sessions setting、YES、Apply 即可，如图 A-1 所示。

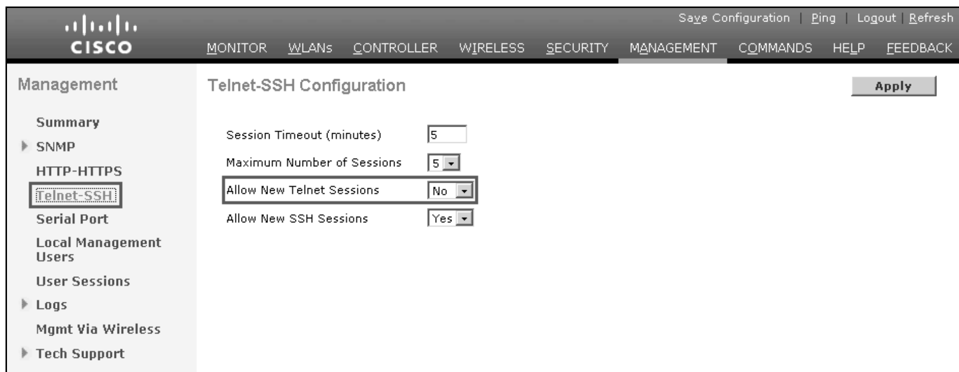


图 A-1　使用 WLC 的 Web 界面允许 Telnet 连接

WLC 的时间必须同升级工具所在的计算机的时钟同步，升级工具配置 AP 产生一个自注册的证书，此证书上有一个基于工具所在机器的时间戳，如果 WLC 的时间同机器时间相差太大，WLC 将会认为证书无效，从而无法完成 AP 到 WLC 的注册。若配置 WLC 的时间，可通过使用 Web 界面，选择 Commands > Set Time 来完成，如图 A-2 所示。

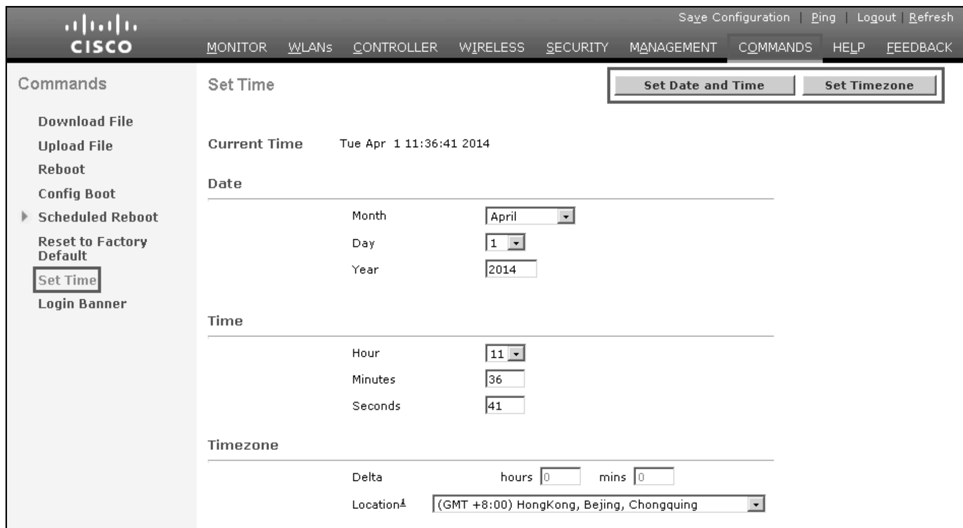


图 A-2　使用 WLC 的 Web 界面配置 WLC 的时间信息

也可以使用命令行通过 config time 来完成。

A.2　升级过程

从自主 AP 升级到轻量级 AP 是通过升级工具来完成的，在升级的过程中，升级工具将会自动关闭 AP 的无线发射，升级工具将会检查如下的几个项目。

① 基本状况检查——是否支持升级 AP 的类型，AP 是否已经运行所需的版本，是否支持无线信号的类型。

② 为自主 AP 升级做好准备——将 PKI 及证书链加入 WLC，以使 AP 能够产生自注册的证书。

③ 加载升级镜像，以便 AP 可以加到 WLC，一旦镜像加载完毕，AP 将执行重启操作。

④ 产生一个输出文件，包含 AP 的 MAC 地址、证书类型和安全密钥 hash，并且自动更新 WLC 内部的信息，输出文件可以导入到 WCS 以便同步到其他控制器。

A.3　安装并运行升级工具必须满足的要求

① 首先以超级用户登录计算机，升级程序只能运行在 Windows 2000、Windows XP 和 Windows 2003 的机器上。

② 升级程序只能升级 Cisco Aironet 1100、1130、1200、1240 及 1310 系列的 AP，AP 必须运行 IOS12.3（7）JA 及以上版本，所有的 AP 必须工作在 AP 模式。

③ 如果升级跨越 WAN 的链路，链路的速率必须大于 128 kbps。

④ AP 和 WLC 必须允许 Telnet 操作。

⑤ 升级工具所在的计算机和 WLC 的时间必须保持同步。

⑥ 在升级时，必须提供一个包含升级 AP 的 IP 地址文件，地址文件中包含有 IP 地址、用户名与密码。对于每一个 AP，IP 地址、用户名、密码和特权密码必须使用逗号分隔，IP 文件中对于同一个 AP 绝不能包含多项。

A.4 安装并运行升级软件 Upgrade Tool

安装好相应升级软件并运行后的界面如图 A-3 所示。

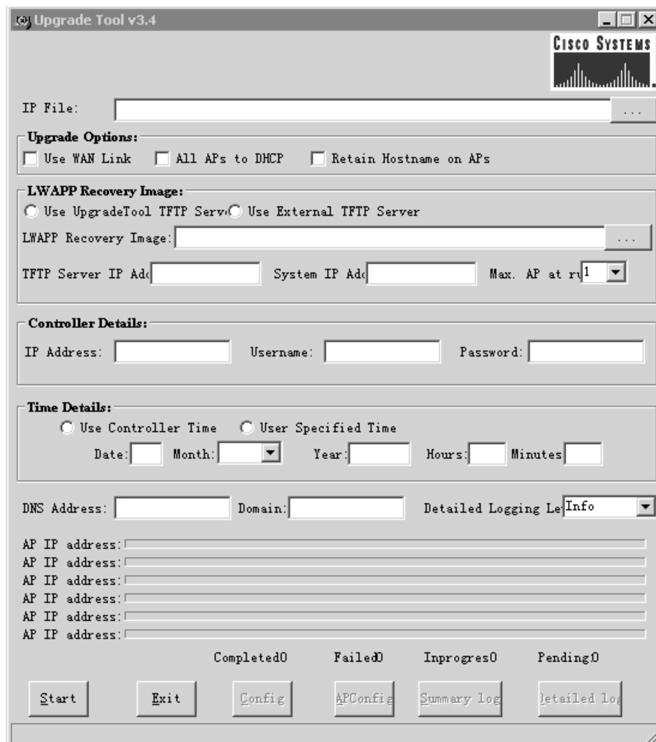


图 A-3 升级工具界面

具体步骤如下所述。

① IP File 字段用来表示输入文件，输入文件包含一个或多个 AP 的信息，文件的格式如下：

```
ap-ip-address,telnet-username,telnet-user-password,enable-password
ap-ip-address,telnet-username,telnet-user-password,enable-password
```

每一行都列出了 AP 的 IP 地址、Telnet 用户名、密码及进入特权模式的密码。

② 指定自主 AP 采用何种方式升级。

Use WAN Link 表示 AP 升级时需要经过 WAN 的线路，如果需要经过 WAN 链路，需要注意如下的事项：

- 如果每次升级 AP 处于不同的 WAN 链路，可以将这些 AP 的 IP 地址放置于同一个配置文件中，当所有需要升级的 AP 处于同一个 WAN 链路上时，不能同时升级这些 AP，以防止出现带宽瓶颈。当使用本地 TFTP 服务器时，传输镜像将会占用大量带宽。
- 如果选择 All APs to DHCP，所有升级后的 AP 将从 DHCP 服务器取得 IP 地址。
- 如果选择 Use External TFTP Server，将会使用 Upgrade Tool 所在工作站之外的 TFTP 服务器。
- 输入映像软件的名称、TFTP 服务器的 IP 地址和本地 IP 地址。

③ 输入控制器的 IP 地址及管理员的用户名与密码。

④ 指定时间：一般是使用控制器的时间。

⑤ 开始升级：升级完成后，将会在安装目录下产生一个文件，文件中包含了证书链等信息，此时需要将此文件导入 WCS 以使升级后的 LAP 能够关联到任一个 WLC。

A.5　IEEE 802.11n AP 的升级

对于 Cisco 1140 和 1250 等 IEEE 802.11n 的 AP，不能通过前面讲到的 Cisco Upgrade Utility 进行升级，此时需要运行一个 TFTP 或者 FTP Server，待 AP 启动完成后，通过有线或无线 Telnet AP 后，使用如下命令进行升级：

```
archieve download-sw /overwrite /reload tftp:/x.x.x.x/image-name
```

当升级完成后，AP 将会自动完成重启，并在控制器完成注册。

附录B >>>

LAP 的注册步骤

本章要点

- LAP 的注册步骤
- 第二层 CAPWAP 发现算法
- 第三层 CAPWAP 发现算法
- WLC 的选举过程

B.1　LAP 的注册步骤

① LAP 发送一个 DHCP 的请求，以便得到一个 IP 地址。

② 如果 LAP 支持第二层的 CAPWAP 模式，LAP 将会在第二层广播一个 CAPWAP 的发现报文，任何一个配置了第二层 CAPWAP 模式的 WLC 在收到此报文后必须发送一个发现应答，除非 WLC 不支持第二层的发现模式。

③ 如果第一步失败或者 LAP 不支持第二层的发现，则进入第三层的发现。

④ 如果第③步失败，则 LAP 将重新启动。

B.2　第二层 CAPWAP 发现算法

第二层 CAPWAP 通信报文可以直接被封装在以太网报文中，虽然在 RFC 的草案中被定义，但是第二层的 CAPWAP 模式在 Cisco 的实施方案中已经逐步被废弃，只有 Cisco 1000 系列的 LAP 可以支持第二层的 CAPWAP 模式，Cisco 2000 系列的 WLC 不支持第二层的 CAPWAP 协议。支持第二层 CAPWAP 发现的 LAP 首先广播一个 CAPWAP 的请求报文，如果本地网络中有支持第二层 CAPWAP 模式的 WLC，控制器将会应答，LAP 将会进入加入 WLC 阶段。

使用 debug CAPWAP events enable 命令可以查看一个使用第二层 CAPWAP 模式的 AP 并加入 WLC 的过程。

加入过程示例如下：

```
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '2'
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery−Response to AP 00:0b:85:51:5a:e0 on Port 2
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:48:53:c0 on port '2'
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:48:53:C0 rxNonce 00:0B:85:51:5A:E0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 CAPWAP Join−Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for
AP 00:0b:85:51:5a:e0（index 48）Switch IP: 0.0.0.0, Switch Port: 0, intIfNum 2,
vlanId 0AP IP: 0.0.0.0, AP Port: 0, next hop MAC: 00:0b:85:51:5a:e0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully transmission of
CAPWAP Join−Reply to AP 00:0b:85:51:5a:e0
```

```
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register CAPWAP event for
AP 00:0b:85:51:5a:e0 slot 0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register CAPWAP event for
AP 00:0b:85:51:5a:e0 slot 1
```

B.3 第三层 CAPWAP 发现算法

如果不支持第二层发现算法或第二层发现模式失败，LAP 将会使用第三层发现算法。第三层发现算法使用不同的选项来发现 WLC。第三层发现算法用来创建一个控制器的列表，当列表创建好以后，LAP 选择一个 WLC 并且尝试加入并关联。第三层 CAPWAP 算法一直重复直到成功找到一个 WLC 并加入。

在第三层 CAPWAP 发现期间，LAP 总是完整运行以下几个步骤来创建一个候选的 WLC 列表。当 LAP 完成了 CAPWAP WLC 的发现步骤后，LAP 将会基于某些策略从候选的 WLC 列表中选择一个 WLC 并发送 CAPWAP 的加入请求。LAP 在从 DHCP 服务器得到 IP 地址后，将会运行发现过程，如图 B-1 所示。

① LAP 在本地 IP 网络上广播一个第三层的 CAPWAP 发现报文，本地网络上任何一个配置了第三层 CAPWAP 模式的 WLC 将会收到此发现请求。

② 任何收到此发现请求报文的 WLC 将会采用单播的形式向 LAP 发送一个发现响应报文。

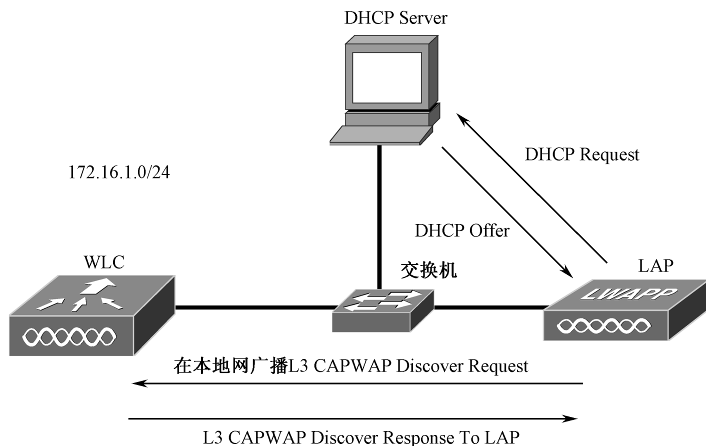


图 B-1 第三层 CAPWAP 发现过程

这里有一个例子，假定 WLC 和 LAP 在同一个 IP 子网 172.16.1.0/16 上，同时有一个 DHCP 服务器的子网，当 LAP 上电启动时，它发送一个 DHCP 的请求报文，当 LAP 取得 IP 地址后，LAP 向本地广播一个第三层的发现报文，因为 WLC 在同一个本地子网上，它将会收到发现请求并回送一个发现响应报文，使用命令 debug capwap events enable 可以展示这个发现过程。

```
（Cisco Controller） >debug capwap events enable
Mon May 22 12:00:21 2006: Received CAPWAP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '1'
Mon May 22 12:00:21 2006: Successful transmission of CAPWAP Discovery-Response to AP 00:0b:85:5b:
fb:d0 on Port 1
```

使用命令 debug capwap packet enable 可以查看报文的实例。

```
（Cisco Controller） >debug capwap packet enable
Tue May 23 12:37:50 2006: Start of Packet
Tue May 23 12:37:50 2006: Ethernet Source MAC（LRAD）: 00:0B:85:51:5A:E0
Tue May 23 12:37:50 2006: Msg Type :
Tue May 23 12:37:50 2006: DISCOVERY_REQUEST
Tue May 23 12:37:50 2006: Msg Length : 31
Tue May 23 12:37:50 2006: Msg SeqNum : 0
Tue May 23 12:37:50 2006: IE : UNKNOWN IE 58
Tue May 23 12:37:50 2006: IE Length : 1
Tue May 23 12:37:50 2006: Decode routine not available, Printing Hex Dump
Tue May 23 12:37:50 2006: 00000000: 00
```

IE 58 用来表示发现的方式，共有以下 4 种：

- 0－broadcast；
- 1－configured；
- 2－OTAP；
- 3－dhcp server；
- 4－dns。

在上例中，值为 0 表示这是一个广播报文。

LAP 同时使用 Over-the-Air Provisioning（OTAP）特性来发现 WLC，OTAP 特性在 WLC 上是默认开通的，OTPA 的发现步骤如下所述。

① 那些已经成功注册到 WLC 的 LAP 可以通过邻居发现协议发送 WLC 的 IP 地址给那些希望获得 WLC 地址的 LAP。

② 希望加入 WLC 的新的 LAP 收到此消息后将会向 WLC 发送一个单播发现请求。

③ WLC 收到此发现请求后将会采用单播发送一个 CAPWAP 的响应报文给 LAP。

建议在 AP 注册时开启 OTPA 功能，待所有 AP 注册完成后再关闭 OTPA 功能。

假定在 172.16.1.0/16 这个子网上，已经有一个注册到 WLC 的 LAP，在 WLC 上开启了 OTAP 功能，当一个新的 LAP 在 192.168.1.0/24 上启动后，它将从 DHCP 服务器获得一个 IP 地址，LAP 然后向本地网络发送一个发现请求报文，因为在本例中，没有本地的 WLC，LAP 将尝试使用 OTAP 来发现 WLC，LAP 侦听邻居的空中报文并获取 WLC 的 IP 地址，新的 AP 向 WLC

发送发现请求报文，WLC 收到请求报文后将发送请求响应报文。

OTAP 发现过程示例如图 B-2 所示。

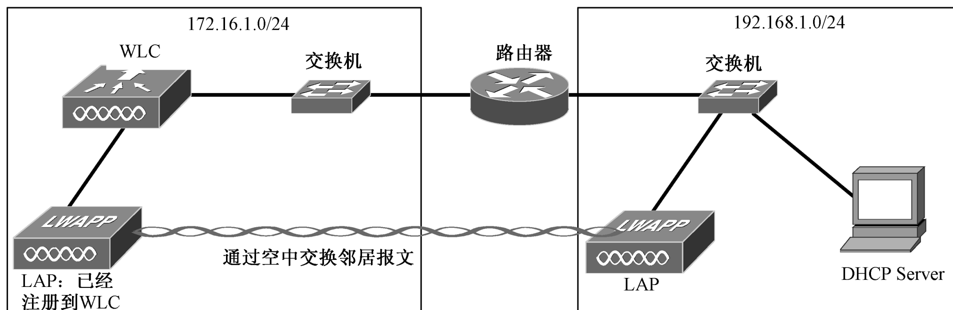


图 B-2　OTAP 发现过程示例

使用命令 debug capwap event enable 可以输出相应报文：

```
Tue May 23 14:37:10 2006: Received capwap DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:37:10 2006: Successful transmission of CAPWAP Discovery-Response to AP
00:0b:85:5b:fb:d0 on Port 1
```

由于 LAP 从邻居报文中知道了 WLC 的确切 IP 地址，LAP 直接向 WLC 发送发现请求，而不是向本地广播一个发现请求报文。

在 debug capwap packet enable 中，IE 58 显示这是一个 OTAP 的发现方式。

```
Tue May 23 14:21:55 2006: Start of Packet
Tue May 23 14:21:55 2006: Ethernet Source MAC（LRAD）: 00:D0:58:AD:AE:CB
Tue May 23 14:21:55 2006: Msg Type :
Tue May 23 14:21:55 2006: DISCOVERY_REQUEST
Tue May 23 14:21:55 2006: Msg Length : 31
Tue May 23 14:21:55 2006: Msg SeqNum : 0
Tue May 23 14:21:55 2006:
IE : UNKNOWN IE 58
Tue May 23 14:21:55 2006: IE Length : 1
Tue May 23 14:21:55 2006: Decode routine not available, Printing Hex Dump
Tue May 23 14:21:55 2006: 00000000: 02 Tue May 23 14:21:55 2006:
```

如果 LAP 在先前的部署中已经注册到一个 WLC，LAP 将会在本地 NVRAM 中维持一个 WLC 的 IP 列表，存储的 WLC IP 列表包含了同一 mobility groups 中所有的 WLC 的地址，下面是发现的过程。

LAP 发送一个单播的第三层 CAPWAP 发现请求给 NVRAM 中保存的每个 WLC，WLC 收到 CAPWAP 的发现报文后将会使用 CAPWAP 的响应报文来应答。下面是一个采用 debug

capwap events enable 和 debug capwap packet enable 命令后的输出案例。

如果使用 clear ap−config ap_name 命令将 LAP 恢复到出厂状态，LAP 所有的配置将会被重置，包括存储在 NVRAM 中的 WLC 的 IP 地址列表，这样 LAP 就需要其他的方法来寻找 WLC 了。

```
（Cisco Controller） >debug capwap events enable
Tue May 23 14:37:10 2006: Received CAPWAP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:37:10 2006: Successful transmission of CAPWAP Discovery−Response to
AP 00:0b:85:5b:fb:d0 on Port 1
（Cisco Controller） >debug capwap packet enable
Tue May 23 14:45:36 2006: Start of Packet
Tue May 23 14:45:36 2006: Ethernet Source MAC（LRAD）: 00:D0:58:AD:AE:CB
Tue May 23 14:45:36 2006: Msg Type :
Tue May 23 14:45:36 2006: DISCOVERY_REQUEST
Tue May 23 14:45:36 2006: Msg Length : 31
Tue May 23 14:45:36 2006: Msg SeqNum : 0
Tue May 23 14:45:36 2006: IE : UNKNOWN IE 58
Tue May 23 14:45:36 2006: IE Length : 1
Tue May 23 14:45:36 2006: Decode routine not available, Printing Hex Dump
Tue May 23 14:45:36 2006: 00000000: 01 Tue May 23 14:45:36 2006:
```

我们也可以使用 DHCP 的 Option 43 选项来返回 WLC 的 IP 地址，下面是发现的过程。

当 LAP 从 DHCP 服务器取得 IP 地址时，LAP 在 DHCP 应答中的 Option 43 字段寻找 WLC 的 IP 地址，LAP 向 Option 43 字段中的每个 WLC 发送一个发现请求，WLC 收到请求后，将向发送 LAP 回送一个发现响应报文。

注释：当 LAP 和 WLC 在不同的子网中时可以使用 DHCP 的 Option 43 字段。

使用 DHCP Option 43 的网络拓扑示例如图 B-3 所示。

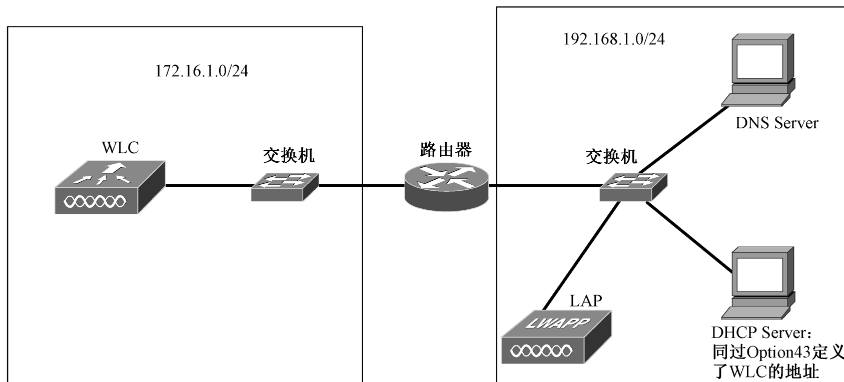


图 B-3　使用 DHCP Option 43 的网络拓扑示例

假定我们在 172.16.1.0/16 网段上有一个 WLC，LAP 和 DHCP 服务器在不同的网段 192.168.1.0/24 上，两个网段之间路由可达，DHCP 服务器已经配置好了使用 Option 43 来提供 WLC 的地址信息。当 LAP 加电启动时，它首先发送 DHCP 请求以便从 DHCP 服务器获得一个 IP 地址，DHCP 应答报文中包含了 WLC 的地址信息，LAP 将向 Option 43 中的每个 WLC 发送一个单播的发现请求，接收到请求的 WLC 将向 LAP 发送发现响应报文，开始整个注册过程。

命令 debug capwap events enable 输出显示了 CAPWAP 序列：

```
Tue May 23 14:43:42 2006: Received CAPWAP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:43:42 2006: Successful transmission of CAPWAP Discovery-Response to AP
00:0b:85:5b:fb:d0 on Port 1
```

从 debug capwap packet enable 命令输出可以看出，采用了 DHCP Option 43 字段来发现 WLC 的地址：

```
Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC（LRAD）: 00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type :
Tue May 23 16:14:32 2006: DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length : 31
Tue May 23 16:14:32 2006: Msg SeqNum : 0
Tue May 23 16:14:32 2006: IE : UNKNOWN IE 58
Tue May 23 16:14:32 2006: IE Length : 1
Tue May 23 16:14:32 2006: Decode routine not available, Printing Hex Dump
Tue May 23 16:14:32 2006:
```

最后，我们也可以使用 DNS 服务器来返回 WLC 的地址，下面是发现的过程：

① LAP 对域名 CISCO-CAPWAP−CONTROLLER.localdomain.进行解析。

② 注意，在 DNS 名称的语法中，localdomain 指需要解析的域名，例如，如果域名为 cisco.com，那么 DNS 的名称就是 CISCO−CAPWAP−CONTROLLER.cisco.com.，AP 需要得到域名的相关信息以便发送相关的域名解析请求给 DNS 服务器。AP 通过 DHCP 的 Option 15 获得本地 DNS 的域名信息。

③ 如果 LAP 能够将此主机名解析成一个或多个 WLC 的 IP 地址，LAP 向每一个 WLC 发送第三层的 CAPWAP 发现请求。

④ 收到发现请求的 WLC 发送一个单播 CAPWAP 的发现响应给 LAP。

这个例子使用同 Option 43 同样的例程，但在这个例子中，DHCP 服务器没有使用 Option 43，但它提供了 LAP 相应的 IP 地址、DNS 服务器的地址以及本地 DNS 的域名信息，客户端得到 DNS 服务器地址后，将向 DNS 服务器发送 CISCO−CAPWAP− CONTROLLER.localdomain.的解析请求，DNS 服务器返回对应的 WLC 的 IP 地址，一旦 LAP 获得了 WLC 的地址，将会发

起向 WLC 注册过程。

使用 debug capwap packet enable 命令表明这种发现方式为 DNS 方式。使用 DNS 发现 WLC 的拓扑示例如图 B-4 所示。

```
Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC（LRAD）: 00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type :
Tue May 23 16:14:32 2006: DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length : 31
Tue May 23 16:14:32 2006: Msg SeqNum : 0
Tue May 23 16:14:32 2006: IE : UNKNOWN IE 58
Tue May 23 16:14:32 2006: IE Length : 1
Tue May 23 16:14:32 2006: Decode routine not available, Printing Hex Dump
Tue May 23 16:14:32 2006: 00000000: 04
Tue May 23 16:14:32 2006:
```

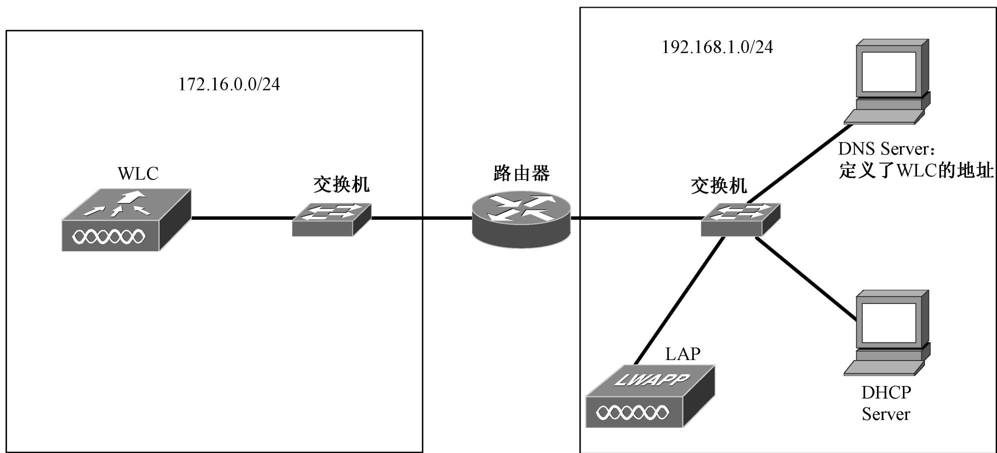


图 B-4　使用 DNS 发现 WLC 的拓扑示例

当 LAP 使用有以上的几种方式发现控制器时都没有收到任何 CAPWAP 的发现响应，LAP 将会自动重启并重复以上的发现过程。

B.4　WLC 的选举过程

当 LAP 完成了以上几种第三层 WLC 发现算法后，LAP 从 WLC 候选列表中选择一个 WLC 并发送 CAPWAP 加入请求，WLC 在发现响应中包含了如下的重要信息：

- 控制器的系统名称（sysName）；

- 控制器的类型（type）；
- 控制器所能支持的 AP 数量以及当前的 AP 负载；
- 主控制器标识（是否为主控制器）；
- AP 管理器（AP-Manager）的 IP 地址。

LAP 使用该信息来进行控制器的选择，采用如下的优先级策略：

① 如果 LAP 先前被配置过 primary、secondary 和 tertiary 控制器，LAP 将检查发现响应报文中的控制器 sysName 字段，以发现 WLC 是否已经被配置成 primary，如果 LAP 发现了匹配的 sysName 的 primary 控制器，LAP 将发送 CAPWAP 加入请求给那个 WLC。如果 LAP 不能发现 primary 的控制器或者 CAPWAP 加入请求失败，LAP 将会尝试匹配 secondary 控制的 sysName，如果匹配成功则发送加入请求，否则继续尝试匹配 tertiary 控制器。

② LAP 将在发现响应中检查 Master Controller flag，如果下面的任何一种假定成立：

- 没有配置任何 primary、secondary 及 tertiary 的控制器；
- 这些控制器不在候选列表中；
- 向这些控制器加入失败；
- 如果某个 WLC 被配置成 Master Controller，LAP 将选择那个 WLC 并发送 CAPWAP 的加入请求。

③ 如果①和②都没有成功，LAP 将尝试加入那些具有最大空闲 AP 数量的 WLC。

LAP 在选择一个 WLC 后，将发送 CAPWAP 加入请求，在加入请求中将内嵌一个 X.509 的证书，如果证书有效，WLC 将会发送一个加入响应用来通知 LAP 加入 WLC 已经成功。WLC 同时在加入响应报文中内嵌自身的证书让 LAP 验证其合法性，当双方证书都验证后，CAPWAP 加入过程结束。

附录C >>>

Windows 2003 Server中DHCP Option 43的创建

本章要点

- 创建供应商类别
- 设置预定义的选项
- 定义Option 43选项

C.1 创建供应商类别

打开 DHCP 服务器管理器工具，右键单击 DHCP 服务器的根并选择“定义供应商类别”Define Vendor Classes，如图 C-1 所示。

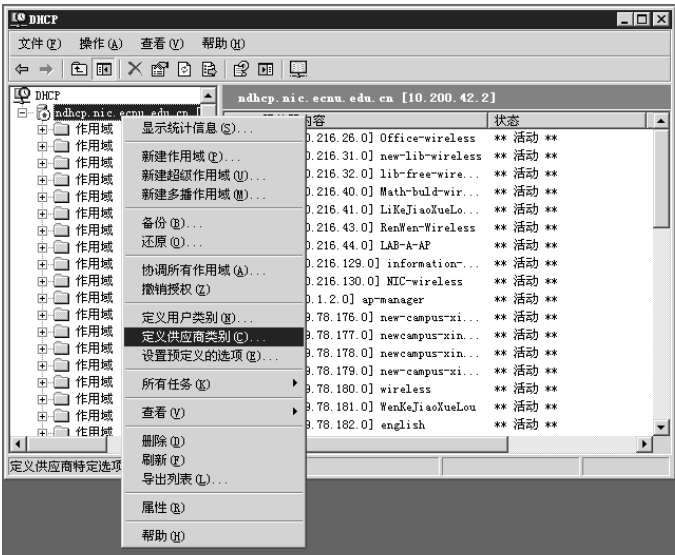


图 C-1 在 DHCP 服务器操作菜单中选择“定义供应商类别”

打开供应商类别的弹出窗口并单击添加，如图 C-2 所示。

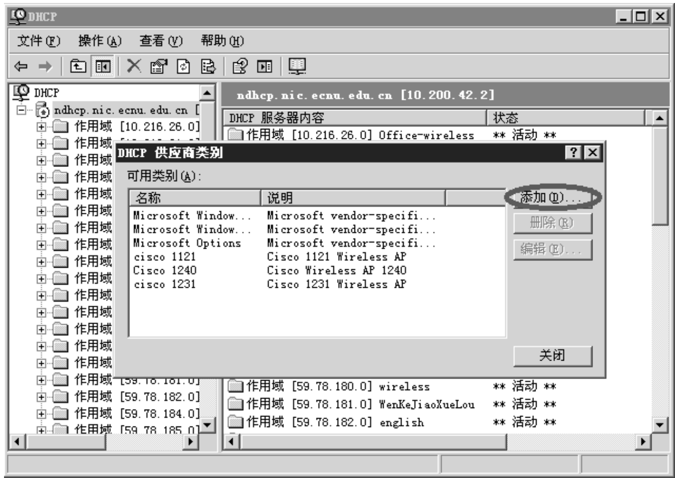


图 C-2 添加供应商类别

在新建类别的弹出窗口中，在显示名称中输入需要显示的名称以及恰当的描述，如图 C-3 所示，在 ASCII 码段，输入正确的供应商字符串值，参见表 C-1 的 VCI 描述，当设置完毕后，单击“确定”按钮并关闭本窗口。



图 C-3　编辑供应商类别

各种 AP 型号的定义如表 C-1 所示。

表 C-1　Cisco 各型号 AP 的 VCI 字符串描述

Access Point	VCI String
Cisco Aironet 1000 Series	Airespace.AP1200
Cisco Aironet 1040 Series	Cisco AP c1040
Cisco Aironet 1100 Serie	Cisco AP c1100
Cisco Aironet 1130 Series	Cisco AP c1130
Cisco Aironet 1140 Series	Cisco AP c1140
Cisco Aironet 1200 Series	Cisco AP c1200
Cisco Aironet 1230 Series	Cisco AP c1200
Cisco Aironet 1240 Series	Cisco AP c1240
Cisco Aironet 1250 Series	Cisco AP c1250
Cisco 3201 Lightweight Access Point（LAP）	CiscoBridge/AP/WGB c3201
Cisco Aironet 1260 Series	Cisco AP c1260
Cisco Aironet 1300 Series	Cisco AP c1310
Cisco Aironet 1520 Series	Cisco AP c1520
Cisco Aironet 1550 Series	Cisco AP c1550
Cisco Aironet 3500 Series	Cisco AP c3500

续表

Access Point	VCI String
Cisco Aironet 3600 Series	Cisco AP c3600
Cisco Aironet 3700 Series	Cisco AP c3700
Cisco AP801 Embedded Access Point	Cisco AP801
Cisco AP802 Embedded Access Point	Cisco AP802

C.2 设置预定义的选项

设置预定义的选项，右键单击 DHCP 服务器的根，并选择“设置预定义的选项”，如图 C-4 所示。

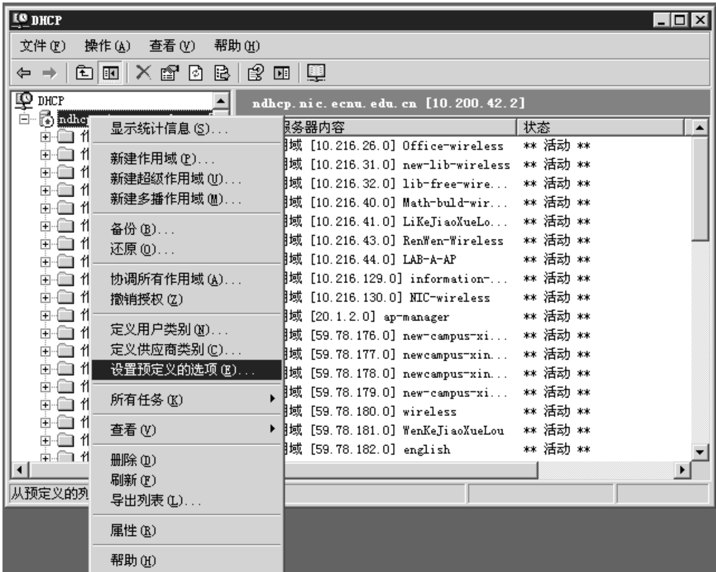


图 C-4 在 DHCP 服务器操作菜单中选择“设置预定义的选项”

使用下拉菜单选择上一步骤中新近创建的供应商类别，选择添加，选项类型窗口将会出现，如图 C-5 所示。

在名称字段，输入一个字符串值，例如，Option 43，使用下拉菜单选择 IP 地址作为数据类型，勾选数组，在代码字段中输入值 241，为之增加一个描述，单击“确定”按钮关闭选项类型窗口，再单击“确定”按钮关闭预定义的选项和值窗口。



图 C-5　设置 Option 43

C.3　定义 Option 43 选项

右键单击服务器选项或作用域选项，并选择配置选项，如图 C-6 所示。



图 C-6　配置作用域的选项

选择高级选项卡，如图 C-7 所示。



图 C-7 编辑 Option 43 种的控制器列表

选择先前定义的供应商类别“cisco 1121”，用户类别请选择“默认用户类别”，选中 241 Option 43 的单选框，并在 IP 地址栏中输入 WLC 的 IP 地址，最后单击“确定”按钮。

采用如上的配置方法，直至将所有类型的 Cisco LAP 都包括。

附录D >>>

采用 Console 口快速部署 LAP

本章要点

- 配置 LAP 的登录用户名及密码
- 配置静态参数将 AP 注册到控制器
- 清除静态配置参数
- 删除 LAP 上的 CAPWAP 配置以便重新部署

在 CAPWAP 模式下的 AP 已经被控制器接管，当需要在远程部署一个 AP 时，AP 通过 WAN 链路连接远程的控制器。当 WAN 链路比较慢以及没有 DHCP 服务器存在时，我们可以手工配置 AP 以让它可以注册到指定的控制器。为了注册到指定的控制器，我们通过 AP 的 Console 口进入特权模式，在特权模式下指定 AP 的静态 IP 地址、掩码、控制器的 IP 地址、AP 的机器名，以及 AP 的默认网关。这些命令能够使我们更加容易地部署 AP，当 AP 处在 CAPWAP 模式下时，这些命令默认是被禁止的；当 AP 运行恢复 IOS 的镜像时，这些命令默认是打开的。

D.1 配置 LAP 的登录用户名及密码

CAPWAP 默认使用 Cisco 作为默认的特权密码，但是为了使能这些命令以便于部署，需要首先提供一个非默认的特权密码，新的密码能够使我们从 Console 口进入 AP 的特权模式。

当从控制器的 Console 口输入如下的命令时，控制器将会发送用户名与密码到 AP：

```
config ap username user-id password pass {AP-name | all}
```

如果输入 *AP-name* 参数，用户名与密码只对指定的 AP 名称生效；如果输入 all 参数，用户名与密码将对所有注册到控制器的 AP 生效。

D.2 配置静态参数将 AP 注册到控制器

使用控制器发送给 AP 的用户名与密码登录 Console 口，进入特权模式，当 AP 运行 CAPWAP 或恢复 IOS 的镜像时，可以静态配置 AP 的 IP 地址、掩码上、默认网关、控制器的 IP 地址，以及 AP 的机器名，命令格式如下：

```
capwap ap ip address ip-addr subnet-mask
capwap ap controller ip address ip-addr
capwap ap hostname ap-hostname
capwap ap ip default-gateway ip-addr
```

当运行 IOS 恢复镜像的 AP 使用静态的控制器 IP 地址注册到指定的控制器后，从控制器下载当前的 CAPWAP 镜像，当 AP 成功注册到控制器后，它从控制器接收配置文件。AP 的静态机器名和控制器的 IP 地址将从 AP 的配置文件中删除，但 AP 自身的 IP 地址、掩码及默认网关则不删除。

当 AP 运行 IOS 恢复镜像时，用于配置静态 IP 地址、控制器地址和 AP 机器名的等命令都是被允许的。

当 AP 运行 CAPWAP 镜像或有一个 CAPWAP 配置文件在 NVRAM 中或者 AP 在控制器上的状态是已注册状态时，以上的命令是被禁止的。当命令被禁止时，如果尝试使用这些命令，Console 上将会返回以下的错误信息：

ERROR!!! Command is disabled.

D.3　清除静态配置参数

为了清除 AP 上静态配置的 IP 地址、控制器的 IP 地址和 AP 的机器名等信息，在 AP 的 Console 端口上输入如下的命令：

```
clear capwap ap ip address
clear capwap ap controller ip address
clear capwap ap hostname
clear capwap ap ip default-gateway
```

当这些命令被禁止时，Console 上同样会返回以下的错误信息：

ERROR!!! Command is disabled.

D.4　删除 LAP 上的 CAPWAP 配置以便重新部署

当我们需要将一个 LAP 从一个地点移到另一个地点时，首先需要删除 CAPWAP 的配置文件，让 LAP 恢复到出厂默认状态。删除 CAPWAP 的配置文件允许使用 AP 的控制口配置静态 IP 地址、控制器地址和机器名的参数，需要删除 CAPWAP 的配置文件。

删除 CAPWAP 配置文件的命令如下：

```
clear capwap private-config
```

这条命令只有在控制器向 LAP 推送新的用户名与密码后才能生效。

如果 LAP 在删除 CAPWAP 的配置文件后由于位置原因重启，用于配置静态参数的命令将会被禁用，在这种情况下，需要首先将此 LAP 加入到控制器，并从控制器上重新推送新的用户名与密码后才能重新配置。

附录E >>>

IEEE 802.11 吞吐量的计算

本章要点

- 无线网络传输开销分析
- IEEE 802.11b 传输性能分析
- IEEE 802.11a 传输性能分析
- IEEE 802.11g 传输性能分析

IEEE 802.11 无线网络已经已经被广泛应用到各行各业，但是在实际应用中用户经常会发现即使在局域网中，应用程序显示的下载速率远远无法达到网卡显示的连接速率，为何会造成此种差异，本节将从理论角度具体阐述无线局域网的实际传输能力。

E.1　无线网络传输开销分析

根据物理层发送机制，虽然 IEEE 802.11b 的传输速率可以达到 11 Mbps，IEEE 802.11g 和 IEEE 802.11a 的传输速率可达 54 Mbps，IEEE 802.11n 的传输可达 300 Mbps。但是根据 IEEE 802.11 协议的传输特性，WLAN 的理论性能（而且是 1 500 Byte 左右的大报文）仅可以达到其传输速率的 50%左右。

首先，我们以一个简单 TCP 报文传输为理论模型分析，一个 TCP 报文传输后需要一个 TCP ACK 来确认（也可能是 Piggy Back 方式的捎带确认）。我们知道，在无线传输中，每个报文传输都要求有一个 ACK 的回应，若发送方没有接收到 ACK，则认为报文已经丢失，需要重传。如图 E-1 所示。

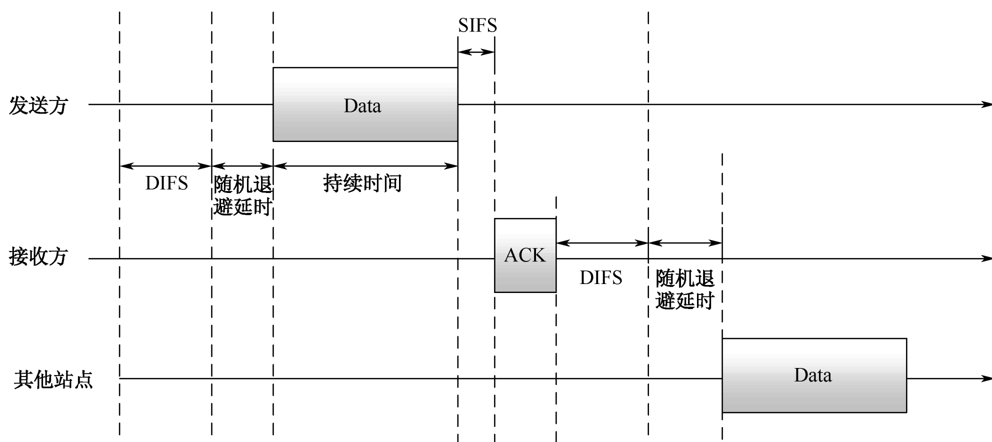


图 E-1　无线报文传输的时序

因为 TCP 传输使用滑动窗口机制，并不是每个报文都需要显式应答，如果不包含 TCP 的应答报文，TCP 报文传输过程如下所述。

① DIFS 延迟：DIFS 时间表示完成一次交互后下一次访问空口的时间。

② 平均回退时间：此回退延时是为了防止多个等待传输的工作站之间同时传输产生冲突。

③ 报文发送延迟：报文经过物理层发送所需要的时间。

④ SIFS 延迟：在报文分片与 ACK 之间的小间隔。

⑤ IEEE 802.11 ACK 帧的发送延时。

因为无线 AP 需要同分布系统进行交互，而分布系统 MAC 帧最大长度一般为 1 500 Byte，

在模型中我们假设MAC层的有效载荷也为1 500 Byte，去除IP头（20 Byte）和TCP头（20 Byte），TCP 报文实际数据为 1 460 Byte。

IEEE 802.11 帧必须通过物理层接口才能传送到空中，这需要物理层在汇聚过程（PLCP）中为每个帧增加前导码和 PLCP 头。而 IEEE 802.11 帧本身就包括 MAC 头，占用 28 Byte。其中还包含了长度为 8 Byte 的 SNPA 标头，因此封装一个数据帧，就会增加 36 Byte 的额外负担。对于 1 500 Byte 的上层报文则变为 1 536 Byte。如果再加上加密标头，MAC 标头的长度就会更长。

较上层协议封包本身是根据所使用的特定物理层规则加以传送的，不同 IEEE 802.11 标准的物理层有其最小块（Block）或符号（Symbol）。速率为 11 Mbps 的 IEEE 802.11b 网络使用长度为 8 位的符号。IEEE 802.11a 和 IEEE 802.11g 所使用的符号可以承载更多的数据，而符号的大小取决于所使用的速率。以 54 Mbps 为例，其使用的符号长度位 216 bit。各种速率之间的差异主要是各个数据块所封装的数据位数不同，与块传送快慢无关。例如，1 536 Byte 的载荷包含了 12 288 bit，对 IEEE 802.11a 而言，此帧需要 57 个连续符号来传递。

数据报文无线传输时间主要包括帧间隔时间和帧传输时间，其中帧间隔包括 SIFS 和 DIFS，另外还要考虑无线的 ACK 帧的传输时间。即传输时间＝DIFS+Backoff + IEEE 802.11 DATA+SIFS+ IEEE 802.11 ACK。其中 IEEE 802.11 ACK 的报文长度位 14 Byte。

E.2 IEEE 802.11b 传输性能分析

IEEE 802.11b 在速率为 11 Mbps 时，其参数取值如下：

- SIFS=10 μs；
- Slot=20 μs；
- DIFS=50 μs（DIFS 为 SIFS 加上 2 时隙）。

长前导码和 PLCP 头传输时间＝144+48=192 μs（前导码以 1 Mbps 速率传输，IEEE 802.11b 前导码和 PLCP 头长度为 192 bit），如果采用短前导码，则 PLCP 头传输时间为 72+48=130 μs

竞争窗口大小为 31～1 023 时隙，每个时隙长度 20 μs，因此为获得最大吞吐量，取退避窗口为 31，则平均退避时间为：

$$20\times\frac{0+1+3+7+15+31}{6}=20\times 9.5=190\ \mu s$$

在 11 Mbps 的速率下，IEEE.11b 使用 8 bit 的符号，每个符号的传输时间为 8 bit/(11 Mbps)=0.73 μs 假设传输 1 500 Byte 的报文，加上 MAC 帧头等信息后为 1 536 Byte，其需要的符号数为 1 536×8/8=1 536 个，而 IEEE 802.11b 的 ACK 报文需要符号数为 14×8/8=14 个。

1 500 Byte 的 IEEE 802.11b 数据发送时间为：192+1 536×0.73=1 313 μs 。

14 字节的 IEEE 802.11b ACK 报文使用 1 Mbps 的基本速率传输，传输时间为：192+14×8/1=304 μs。

合计传输时间为：50+190+1 313+10+304＝1 867 μs。

因此，传输 1 460 Byte 的 TCP 数据需要 1 867 μs，其有效传输速率为：

1 460×8 bit/1 867 μs =6.26 Mbps

E.3　IEEE 802.11a 传输性能分析

IEEE 802.11a 工作在 54 Mbps 时，其参数取值如下：

- SIFS=16 μs；
- Slot=9 μs；
- DIFS=34 μs （DIFS 为 SIFS 加上 2 个时隙）；
- 前导码和 PLCP 头传输时间＝20+4=24 μs（前导码以 1 Mbps 速率传输）。

竞争窗口大小为 15~1 023 时隙，每个时隙长度 9 μs，为获得最大吞吐量，取退避窗口为 15，则平均退避时间为：

$$9\times\frac{0+1+3+7+15}{5}=9\times5.2=46.8\ \mu s$$

在 54 Mbps 速率下，IEEE 802.11a 使用 216 bit 的符号，每个符号的传输时间为 216 bits/(54Mbits/s)= 4 μs，假设传输 1 500 Byte 的报文，加上 MAC 帧头等信息后为 1 536 Byte，其需要的符号数为 1 536×8/216=57 个。

1 500 Byte 的 IEEE 802.11a 数据发送时间为：57×4=228 μs。

14 Byte 的 IEEE 802.11a ACK 报文使用 24 Mbps 的基本速率传输（IEEE 802.11a 的基本速率为 6 Mbps、12 Mbps 与 24 Mbps，假设 ACK 以最大的基本速率传输），传输时间为：24+14×8/24=28.7 μs。

合计传输时间为：34+46.8+24+228+16+28.7＝377.5 μs。

因此，传输 1 460 Byte 的 TCP 数据需要 377.5 μs，其有效传输速率为：

1 460×8 bit/377.5 μs =30.9 Mbps

E.4　IEEE 802.11g 传输性能分析

IEEE 802.11g 工作在 54 Mbps 时，其参数取值如下所述。

- SIFS=10 μs；
- Slot=9 μs（工作在非保护模式下）；
- DIFS=28 μs（DIFS 为 SIFS 加上 2 个时隙）。

为了同 IEEE 802.11a 取得相同的速率，还有 6 μs 的扩展时间。

前导码和 PLCP 头传输时间＝72+20=92 μs（前导码以 1 Mbps 速率传输，假设使用短前导码）。

竞争窗口大小为 15~1 023 时隙，每个时隙长度 9 μs，为获得最大吞吐量，取退避窗口为

15，则平均退避时间为：

$$9 \times \frac{0+1+3+7+15}{5} = 9 \times 5.2 = 46.8\ \mu s$$

在 54 Mbps 速率下，IEEE 802.11g 传输 1 500 Byte 的报文，加上 MAC 帧头等信息后为 1 536 Byte，其需要的发送时间为 1 536×8/54=228 μs。

14 Byte 的 IEEE 802.11a ACK 报文使用 24 Mbps 的基本速率传输（IEEE 802.11b 的基本速率为 1 Mbps、2 Mbps、5.5 Mbps、11 Mbps、22 Mbps、33 Mbps，假设 ACK 以最大的基本速率传输），传输时间为：92+14×8/33=95 μs。

合计传输时间为：28+6+46.8+92+228+16+95＝511.8 μs。

因此，传输 1 460 Byte 的 TCP 数据需要 501 μs，其有效传输速率为：

1 460×8 bit/511.8 μs =22.82 Mbps

由此可见，虽然 IEEE 801.11g 和 IEEE 802.11a 都以 54 Mbps 的速率运行，但由于 IEEE 802.11g 需要兼容 IEEE 802.11b，产生了大量的额外开销，吞吐量也比 IEEE 802.11a 有明显的下降。

以上的论述因为没有考虑 TCP 传输中 ACK 报文的时间，因此，在实际使用中，如果考虑 ACK 的报文，吞吐量可能还要更低。

附录 F >>>

术语及缩略语

术语 / 缩略语	描　　述
CAPWAP	Control And Provisioning of Wireless Access Points——AP 和无线网络控制器之间的控制及数据隧道协议
WLAN Controller/Controller/WLC	Wireless LAN Controller——对所有的轻量级 AP 进行集中以及统一管理，使他们之间形成一个完整系统
Access Point/AP/WAP	Access Point——一种智能桥设备，为无线设备提供网络接入功能，有时 AP 也称为 WAP，Wireless Access Point
Lightweight Access Point/LAP	能够运行在 Cisco 统一无线网络体系之下，LAP 和 WLC 之间采用 CAPWAP 进行通信
Autonomous AP	一个传统的 AP，不需要无线网络控制器的支持
WCS	Wireless Control System——用来管理 Cisco 无线控制器及轻量级 AP 的软件系统，能够对 Cisco 无线网络进行全方位管理
ACS	Access Control Server——Cisco 的 AAA 服务器，能通为 Cisco 的无线网络提供 RADIUS 等多种认证方式
WLAN	Wireless Local Area Network，无线局域网
IEEE 802.11 WLAN	在物理层和 MAC 层运行 IEEE 802.11 协议的无线网络
CUWN	Cisco Unified Wireless Network——Cisco 统一无线网络
Wireless Station/Wireless Client	连接到 IEEE 802.11 无线网络的无线用户端设备
SSID	Service Set Indentifier——服务集标识，用来区分不同的无线接入网络，最多可以有 32 个字符

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传　　真：（010）88254397

E-mail：　dbqq@phei.com.cn

通信地址：北京市万寿路173信箱

电子工业出版社总编办公室

邮　　编：100036